区块链电信行业应用白皮书

(1.0 版)

2019 年 5 月

可信区块链推进计划

版权声明

牵头单位及牵头人:

中国移动通信有限公司研究院　　郭漫雪
中国电信北京研究院　　梁伟
中国联合网络通信有限公司　　王志军

主要编写单位及编写组成员:

中国电信北京研究院　　赵君
中国移动通信有限公司研究院　　黄更生、王青、李亚强、彭晋、阎军智
中国联合网络通信有限公司　　王蓉
中移信息技术有限公司　　彭伟军、聂磊、夏嘉
中国联通网络技术研究院　　薛淼、刘千仞
中国联通北京规划设计院　　夏俊杰、孙晔
中兴通讯股份有限公司　　郑锦荣、胡宪利、黄峥、王海峰、纪竹亮、章坚、张再军
华为技术有限公司　　李汉国、杜伟、窦圣跃、张亮亮、张小军、刘再耀
北京华麒通信科技有限公司　　张隽辉、应文池

联动优势科技有限公司　　殷舒
杭州趣链科技有限公司　　陈晓丰、徐立家
智链万源（北京）数字科技有限公司　　董宁

支持单位：

中国信息通信研究院
深圳市网心科技有限公司
全链通有限公司
北京太一云技术有限公司
微位（深圳）网络科技有限公司

序　　言

当前，新一轮科技革命和产业变革席卷全球，大数据、云计算、物联网、人工智能、区块链等新技术不断涌现，数字经济正深刻的改变着人类的生产和生活方式。区块链作为一项颠覆性技术，正在引领全球新一轮技术变革和产业变革，推动“信息互联网”向“价值互联网”变迁。区块链应用可以为实体经济“降成本”、“提效率”，助推传统产业高质量发展，加快产业转型升级。同时区块链应用正在衍生为新业态，成为经济发展的新动能。

区块链对于电信运营商来说，既是挑战，也是机遇。区块链的去中心化、防篡改以及多方共识机制等特点，决定了区块链在解决电信行业合作中需要多方共同决策并建立互信的问题、优化运营商间及与上下游产业链的合作协同等方面具有重要的价值。基于区块链的新商业模式可能改变现有的电信价值链，但其创造新的商业模式可能将革新现有商业模式，提升效率、降低成本并带来新的收入。

该报告第一章介绍了区块链技术的起源以及区块链技术国外内电信领域发展现状。第二章围绕区块链基本原理、关键技术、区块链意义和价值展开深入分析。第三章从发展现状、解决方案、发展策略三个方向入手，详细探讨了电信设备管理、动态频谱管理与共享等八个区块链电信行业应用。

目 录

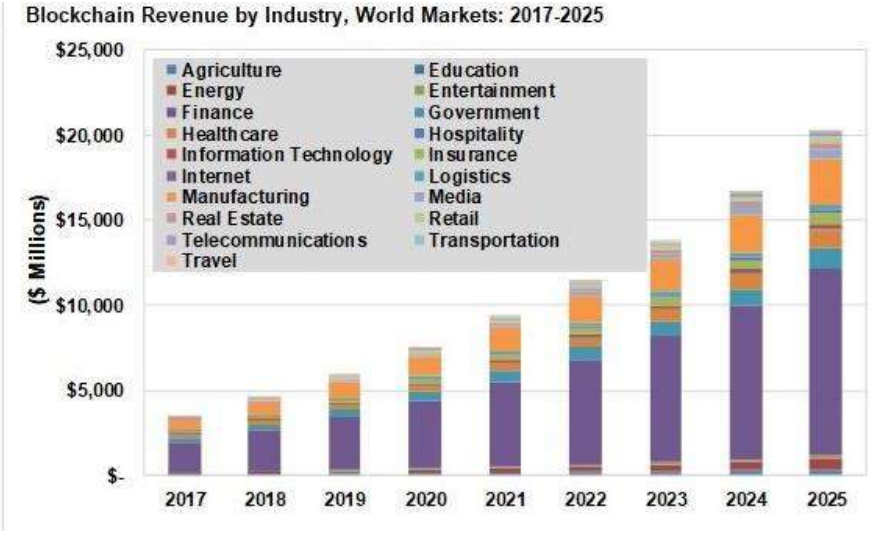
一、概述

（一）区块链技术起源和产业现状

区块链概念最早出现在中本聪的比特币白皮书中，但并非以“区块链”的提法出现，而是以“工作量证明链”的形式陈述的。2008 年 11 月 1 日，中本聪发表《比特币：一种点对点的电子现金系统》一文，阐述了基于 P2P 网络技术、加密技术、时间戳技术、区块链技术等的电子现金系统的构架理念，标志着比特币的诞生。2009 年 1 月 3 日第一个序号为 0 的比特币创世区块诞生，2009 年 1 月 9 日出现序号为 1 的区块，并与序号为 0 的创世区块相连接形成了链，标志着区块链的诞生。

在产业方面，过去三年，位于硅谷和纽约的区块链技术公司成为了各风投基金竞相追捧的热门项目。麦肯锡的研究表明，区块链技术是继蒸汽机、电力、信息和互联网科技之后目前最有潜力触发第五轮颠覆性革命浪潮的核心技术。当前企业区块链正在承载商业流量，并且正在超越概念，降低成本则是部署的主要动力。未来将出现由该技术实现的新业务模型，其好处来自于替换中介并通过“智能合约”的业务规则来实现自动化和验证事务。

以下为不同研究机构对区块链市场未来规模的预测分析：Tractica 预测，2018 年全球企业区块链市场在 46 亿美元左右，到 2025 年市场规模将达到 203 亿美元；据 Research and Markets 据测，到 2022 年，全球区块链市场规模将达到 139.6 亿美元。2017 至 2022 年间，该市场的年复合增长率为 42.8%。



资料来源：Tractia

图 1：2017-2025 全球区块链产业收入情况

（二）电信领域区块链发展现状

1. 国外电信领域布局区块链现状

正如互联网所给我们带来的一样，区块链已经不仅仅是一项技术、一种工具，更是一种思维方式，区块链作为一种新型的技术组合，其去中心化、难以篡改、不可抵赖等特点不仅为电信行业带来了一种全新的信用模式，也使其数字服务更具竞争力，进而帮助电信行业降低成本，为该领域带来了全新的视角。目前，国外电信运营商布局区块链技术主要有三种方式，分别为直接投资、联盟合作和自主研究三种方式，并已在一些电信领域服务场景中取得一定的成果。

最早尝试电信运营领域的是美国电信巨头 AT&T，当时申请一项关于使用区块链技术创建家庭用户服务器的专利。该专利成为了电信行业在区块链领域的首个应用探索；随后法国电信 Orange 也选择在金融服务领域尝试区块链，用于自动化和提高结算速度，从而在一定程度上减少了清算机构的成本。

2017 年 9 月瑞士大型国有电信供应商 Swisscom 宣布成立“Swisscom Blockchain AG”公司，该公司专注于围绕区块链技术开展的一系列服务，包括面向企业的解决方案。

2017 年 9 月美国电信运营商 Sprint、美国加州区块链初创公司 TBCASoft、日本软银集团、台湾远传电信（“Far EasTone”）合作成立 CBSG 运营商区块链联盟（Carrier Blockchain Study Group），该联盟旨在共同构建跨运营商的全球区块链平台和生态，进而为电信成员及其客户提供跨运营商的各种服务，如在跨运营商的支付平台系统上完成充值、移动钱包漫游、国际汇款和物联网支付等。

2018 年 5 月西班牙电信巨头 Telefonica 宣布，该公司正在和安全技术创业公司 Rivetz 合作，开发基于区块链交易和即时通讯的智能手机解决方案。双方将把 Telefonica 公司的网络安全服务与 Rivetz 的区块链及可信计算技术(trusted-computing)结合到一起，以此探索去中心化的解决方案所具备的安全性和数据控制能力。该项工作将专门用于改进讯息通信和加密货币钱包应用程序的安全度。

2. 国内电信领域区块链技术发展现状

目前，国内电信行业中的很多公司已在不同程度上涉足于区块链技术领域，并与有关方面达到了合作共识。他们不仅大力推动区块链标准的国际化，还不断深入探索，挖掘区块链的应用场景，切实结合行业特点，积极研发基于区块链技术的电信领域应用平台，用于解决电信行业现存难题，从而共同推动区块链在电信应用场景的真实落地，共同营造与建立电信领域新的行业生态。

中国电信打造的区块链可信基础溯源平台“镜链”，提供完备的区块链溯源基础能力，荣获 2018 中国“双创”好项目奖；此外，其自研的基于区块链去中心化的 IOT 平台，整合了中国电信政企网关资源，构建了去中心化的共享经济平台，最大程度上保证了用户数据安全与设备控制安全。在标准方面，中国电信牵头在 ITU-T SG16 成立了首个分布式账本国际标准项目，即：分布式账本业务需求与能力。

中国移动积极推动 ITU-T 成立“区块链（分布式账本技术）安全问题小组”并担任副组长职务，该组致力于区块链安全方面的研究和标准化；此外，中国移动在 GSMA 的欺诈与安全工作组(FASG, Fraud and Security Group)立项研究区块链应用于运营商 PKI 领域的标准工作。中国联通联合中兴通讯、信通院、中国移动在 ITU-T SG20 建立了全球首个物联网区块链国际标准项目“基于物联网区块链的去中心化业务平台框架”;中国联通、中国电信和中国移动共同在 ITU-T SG13 发起“NGNe 中区块链场景及能力要求”，研究区块链在电信网络中的应用。

2017 年 5 月，中兴在中国国际大数据产业博览会上推出了中兴 uSmartInsight 区块链解决方案，即下一代电子证照共享平台，为践行“互联网+政务”提供完善可靠的政务信息系统整合共享方案。

2017 年 10 月，中国信息通信研究院和中国人民银行数字货币研究所联合代表我国产业界向 ITU-T 分布式账本焦点组提交了《可信区块链：一个分布式账本技术评估框架》技术提案，这对于我国下一步在区块链国际标准制定中的作用意义重大。

2017 年 12 月，浪潮集团推出了国内首家也是目前国内唯一一家基于区块链技术的质量提升服务平台——质量链。该质量链已经成为国内领先的质量提升线上服务基础设施，得到了各地方政府、企业、检测机构、消费者的多方认可。

2018 年初，华为公司发布了华为云区块链服务 BaaS 平台,该服务是基于开源区块链技术和华为在分布式并行计算、PaaS、数据管理、安全加密等核心技术领域多年积累基础上推出的企业级区块链云服务产品，同年 4 月，在 2018 华为全球分析师大会上，华为发布了《华为区块链白皮书》，计划未来从在远程医疗、食品溯源、车联网多个应用场景进军区块链领域。

从上述可见，目前，国内外电信企业在区块链领域均积极展开布局，抢占区块链标准高地，加快区块链技术研发投入、加强应用试点示范，加大曝光率和影响力，并加强多方合作，建立行业生态。但各家并未盲目跟风，因为区块链对于电信运营商来说，既是挑战，也是机遇。各国运营商都期待在新一轮的技术革命浪潮中抓住战略机遇，从而掌握区块链技术发展的主动权。谁将成为区块链赢家，让我们拭目以待。

二、区块链基本介绍

（一）基本原理

区块链是英文“Blockchain”的翻译，这是一个合成词，原始的意思是由多个区块组成的链。每个区块包含链上前一个区块内容计算

出来的哈希值，修改任何一个区块的任意一个字符都能导致后续计算出来的哈希值和下一个区块记录的不匹配，很容易被别的节点检测出来，只有修改了链上后续所有区块的内容才能保证区块链的完整性，这是一个成本极高或者不可能完成的事情，保证了数据的不可篡改性。

区块通常包含多个交易，交易代表的是某个具体操作或者操作的结果，是区块链最小的组成单元。当然，在某些特殊的架构设计里，交易还可以包含多个操作，可以任意指定组合顺序，形成一个分布式事务，共同构成最终的交易。根据共识算法的不同，交易包含的内容可能是不同节点达成共识的结果，也可能是某些节点先打包进区块还需要其他节点共识确认。

区块链表达的是一种数据结构，怎么把多个区块组织存储起来，用的是数据结构里最为经典的链表结构。如今的区块链已经演变出了多种数据结构，比如采用图形的数据结构 DAG（Directed Acylic Graph），已经有多个项目采用了类似的方法，比如 IOTA、Byteball 等，还有一些项目并不显示的关联各个区块，而是直接存储起来，比如 Corda 就没有链式或者图形的数据结构，同样可以实现数据不可篡改的特性。

（二）区块链关键技术

区块链的不可篡改性是通过密码学保证，包括了常见的密码学算法种类，哈希算法、对称加密算法和非对称加密算法等。哈希算法是通过算法对数据的内容计算摘要，得到一个固定长度的字符串，一般

情况下哈希计算得到的摘要比原始数据长度短的多，相同的数据经过相同的哈希计算能得到相同的摘要，所以可以在只存储摘要的情况下，验证原始数据的完整性。同时，在没有找到碰撞的情况下，哈希计算是一个不可逆的过程，公开和存储摘要并不会泄露原始数据的内容。哈希计算有多种用途，区块默克尔树根的计算通常是对区块包含的交易计算哈希得到的，能够快速验证区块内容是否被修改过。结合非对称加密，对数据进行哈希计算后的摘要利用私钥进行加密计算后得到数字签名，作为签名者对数据内容确认的凭证。签名私钥是签名者自己保管的，只能自己才能进行加密，通过签名私钥对应的公钥解密以后得到签名者哈希计算出来的摘要，验证者按照相同的哈希算法计算新的摘要，查看是否匹配就能验证是否是正确的签名，并且签名者已经签名的事实是不可抵赖的。非对称加密能够对数据进行加密，性能一般较差，通常需要结合对称加密对原始数据进行加密，保证链上数据的隐私性。隐私保护有多种方法，分为物理隔离和逻辑隔离，物理隔离是把数据分开存储，从物理上保证数据的隐私，这是一种安全级别更高的做法，比如 Hyperledger Fabric 的多通道技术，就是只有加入到特定通道的节点才会同步链上的数据。也不是所有的数据都能通过物理隔离的方法实现，在同一个链上的数据还需要有隐私保护的需求，群签名、环签名、零知识证明、同态加密、多方计算等是目前研究和使用较多的技术。

通常，节点只信任本地运行的程序和存储的数据。多个节点同时

拥有完整的账本拷贝就成了共享账本，同时篡改所有节点的账本难度比修改单个节点的账本难度要高很多，这也是区块链具有不可篡改性的根本原因。节点之间如何维护相同的账本是共识机制来保障的，包含了多个方面的内容，节点之间如何确认数据、节点之间如何同步数据、节点如何验证数据是有效的。不同的节点会收到不同的数据，这些数据能否按照相同的逻辑顺序确认数据或者执行程序是共识算法实现的。共识算法有多种分类方法，按照共识以后是否是最终确定性结果可以分为大概率一致的共识算法和绝对一致的共识算法，按照是否允许拜占庭容错可以分为 BFT 和 CFT 的共识算法。共识达成一致的结果需要在全网节点进行同步，为了提高同步的效率，通常会采用 P2P 的方式进行传输。接受到数据的节点验证通过以后才记录到本地账本中。

在共享账本的基础上，智能合约是区块链发挥更大价值的核武器。运行智能合约的节点基于相同的数据输入执行相同的业务逻辑，在没有不确定因子的情况下会得到相同的数据输出。利用这种机制，各个节点可以独立的执行智能合约，确认是否能够达成共识，或者对执行的过程进行回放，验证执行结果的有效性。智能合约本身是应用程序，之所以称为智能合约，是有两方面的原因，首先是这些应用程序是多个节点共享的相同的拷贝，所以又被称为合约代码，其次是这些应用程序是基于某个特定的链，运行在安全的环境中，包含了访问链上数据的接口，也只能通过这些接口才能写入数据，最终在多个节点之间达成共识。从运行机制上来说，智能合约有基于虚拟机的形态，智能

合约代码会翻译成虚拟机可解析的字节码解释运行，以太坊的 EVM 和 Corda 的 JVM 都是这种类型；也有基于容器沙箱运行的形态，这种形态可以提供多中语言的开发接口，实现和账本的交互，Hyperledger Fabric 就是基于 Docker 容器提供的安全隔离环境运行智能合约的。

（三）区块链意义和价值

区块链并非是完全新兴的技术，利用了原有的技术体系，基于密码学体系构建的共享账本，给区块链各参与方协作提供了全局数据视图的基础，每个区块链参与方节点能够信任本地的账本和更新账本的智能合约，通过技术的手段和机制，信任各个参与方共识的结果，进而信任链上节点的行为和数据，共同构建一个信任的社会。

1. 信任能够让不能做的事情变得可能。

对于资金的安全和数据的隐私保护是基本的需求，在没有确保这些基本保障的情况下，机构和个人都会倾向于保守的做法，规避未知的风险。区块链技术把原本隔离的交易方凝聚到一起，根据自己的利益诉求共同制定规则和遵守规则，创建一个安全可信的环境，在每个参与方都认为安全可控的状态下，更容易探索和尝试一些可能性，这种内生的安全感，拉近了各方的距离，搭建了一种信任的桥梁。

2. 信任能够让高成本的事情降低门槛。

在缺乏信任的体系下，需要参与协作的各个参与方通常都会各自设置自己的安全边界，定义安全边界内允许的行为，并制定各种不同

级别的规则来保障交易的顺利进行，单纯为了信任就会付出高昂的成本，由此，信任成了一种奢侈品，有的时候可遇不可求。在区块链的世界里，信任是底层基础设施里内置的属性，所有的参与方只需要关注核心的业务功能，极大的简化了交易的模式，降低交易的门槛。

3. 信任能够让长周期的事情变得高效。

信任交易模式下，不必要的一些流程就简化了，所有参与方按照相同的规则运行，明确了各自的职责和期望的反馈，把人为参与的操作缩减到机器的自动执行，能够让人为共识延迟的量级减少到网络延迟的量级，运算速度的对比差是显而易见的了。

4. 信任能够让小范围的事情扩大规模。

区块链制定的规则对所有的参与方都是透明清晰的，共同约定共同遵守共同执行，所有的潜在参与方都能依赖这样的规则，根据各自的需求参与到区块链建设中来，贡献或者获取都能得到认可，简单可扩展的模式才能快速复制，形成规模效应，覆盖和影响更多的机构和个人。

5. 信任能够让随意的事情变得有粘性。

在面临众多的选择时，每个参与方一定是选择对自己有利的那一个，区块链的简单可依赖，会形成思维的惯性，影响到决策的行为，这会是一个思维模式的转变。当这种原本随意的选择趋同的时候，这种行为的粘性就体现出来了。

在信任的基石上，区块链会融入到所有的活动中，不管是企业和企业之间，还是企业和机构个人之间，能够让社会变得更真实，更美好。

三、区块链电信行业应用场景及方案

为了进一步挖掘区块链在数字资产、电信资产、新一代网络建设等运营商相关领域的应用价值，本章从业务管理、业务服务、网络运营三个方面筛选出八个相关应用场景，如图 2 所示，除此之外，本章深入分析了相关领域当前发展现状，同时提出基于区块链实现的解决方案以及未来发展策略。

图 2 场景架构图

（一）电信设备管理

1. 发展现状

电信运营商网络中存在大量硬件设备，广泛分布于核心网、传输

网、数据网、接入网等多个领域。一方面电信设备数量多、种类多、厂家多、批次多，部署于以百计的数据中心及端局机房，虽然存在集中化的统计型设备资产管理方式，但是难以形成自顶向下透明化穿透式的管理及设备管理的全局视图，也无法形成对特定电信设备的全生命周期管理。另一方面，电信设备巡检方式仍处于数字化/智能化转型过程中，巡检数据的自动采集、可信存储、记录溯源、智能分析等全流程技术仍不完备。 因此，电信设备管理面临穿透式管理及高效巡检等痛点问题。

2. 解决方案

针对目前电信设备管理与设备巡检的现状及痛点，本方案结合多种前沿技术，设计实现一个高效、智能、透明的电信设备管理平台。电信设备管理平台基于区块链作为底层数据存储，利用区块链数据可靠、可信等特征，结合物联网、大数据、人工智能等技术，为电信运营商提供设备巡检和设备全生命周期管理服务，以提高巡检质量和效率。

图 3 电信设备管理平台的功能架构图

电信备管理平台的功能架构图如 3 所示。整体上，电信设备管理平台的参与方有运营商集团、各省市分公司。省市公司按照要求对设备进行巡检，记录在区块链上；集团获取链上的可信数据，实时检查设备巡检工作的落实情况。同时电信设备管理平台通过接口与运营商的业务系统进行交互，实时同步设备故障信息以及设备风险信息，助力提高业务处理效率。

具体而言，电信设备如传输线路、业务系统支撑设备、基站及配套等设备的详细信息，采用统一数据结构，保存在区块链的设备链中。链上的设备信息在全网节点中进行共享，便于设备信息的使用及对其进行统计查询等。不同省份通过不同的设备巡检子链，保存所维护设备的巡检数据。

其中，巡检数据通过人工采集和自动感知两种方式进行获取。人工采集是运维人员携带定制化的移动终端，前往巡检现场进行数据采集。移动终端具备移动通信、近场通信、GPS 定位、拍照、信息录入等功能，可收集温度、湿度或设备现场照片等巡检内容，也可记录运维人员的运动轨迹，保障巡检质量。自动感知方式，是指在巡检现场安装相应设备，结合物联网技术，对巡检数据进行自动感知，并实时地将收集到的数据上传。如在巡检现场安装温度、湿度传感器或摄像头，获取巡检数据，收集环境数据，或是利用探测器定时对设备进行拨测，检测设备运行状态。

同时，根据电信公司历史运行情况、月初月末交易峰值、地域特征等建立数据模型，结合深度学习技术，预测故障设备；深度学习的

结果能够持续验证、回归、完善数据模型，优化巡检工作。

此外，区块链所存放的数据，开放给集团公司、省公司进行查询、统计。集团公司可根据这些数据，对各省公司、地市公司的工作质量进行监督，也可根据链上数据统计出巡检覆盖、巡检频率、巡检质量、故障数量、故障率及故障处理等多种指标，用以评价巡检工作质量。

本方案对电信运营中所涉及的设备进行管理。同时，囊括了电信行业设备管理及巡检的流程，通过建设统一的电信设备管理系统，实现对设备维护工作的规范化、标准化和精细化管控。方案价值主要体现在以下几个方面。

1) 提升巡检效率。本方案不但兼容以往人工巡检方式，还支持自动巡检方式，对接传感器、摄像头、探测器等，无需人工接入，快速对巡检数据进行采集。
2) 降低人工成本。通过大数据及深度学习等技术，优化巡检计划，制定最优巡检周期，减少重复巡检。使用移动终端扫描二维码或近场通讯方式读取数据，比填写纸质表单更加节省时间。
3) 提升巡检质量。采用自动化巡检数据采集模块，降低了人工处理产生错误的概率，提高巡检数据的准确性。同时，通过人工智能技术，有效识别高危系统及设备，提前排查，重点巡查，进一步提升巡检工作效果。
4) 提供统一的设备管理与巡检解决方案。电信设备种类繁多，本方案提取设备关键信息，在集团公司内对同类型设备构建统一数据模型，保证设备管理的一致性与规范化。

5）促进巡检工作良性展开。区块链公开透明，各机构能够通过区块链查看彼此工作情况，起到相互促进的作用。同时，区块链上保存的数据难以篡改，能够准确体现巡检工作进展及完成情况，便于对巡检工作的监督及质量管理。

6）可定制，可兼容各省公司的差异性。各省公司的巡检、工单等数据保存在不同链中，各省可根据实际情况，制定不同巡检模板或工单模板，从而满足各省公司的定制化需求。

3. 发展策略

基于区块链的电信设备管理方案，预计将经历三个发展阶段，如下图 4 所示：

图 4 三个发展阶段

第一阶段，链化建设。主要完成电信设备/用户巡检行为与区块链基础设施之间的数据打通，实现电信设备上链、用户巡检行为上链、巡检信息上链等，形成电信设备及巡检管理的全局视图。通过在区块链系统之上构建电信设备管理平台及设备巡检和监督的全流程管理，对电信设备形成自顶向下穿透式管理，便于对设备进行全局管理和调

度；对巡检数据进行可靠记录，从而对巡检行为和巡检质量进行监督等。

第二阶段，自动化建设。通过融合物联网技术，实现巡检数据的自动采集，将巡检方式扩展为自动化检查，提升巡检效率。具体的，巡检员可通过移动终端 NFC 识别、扫描设备二维码等保证录入数据来源的真实性，也可通过实时定位的方式，对巡检工作进行打卡验证。除此以外，对于设备资产较重的企业，可以将电信设备管理平台与设备管理系统对接，将设备采购、入库、上架、维修、下架等数据进行上链，对设备进行全生命周期管理，从而优化采购策略、提升设备使用效能。

第三阶段，智能化建设。基于区块链登记的设备、巡检及运行数据，结合大数据技术，建立数学模型，并通过深度学习算法对模型持续改进，从类型、厂商、批次、型号、年限等多个维度对设备运行状况实施精准分析和预测，对设备使用及调度进行全局管理，对设备运行风险进行高效预警，对设备巡检质量进行有效监督。同时，对巡检范围进行横向拓展，包括但不限于电信设备巡检、生产设备巡检、测试仪表设备巡检、仓库盘点、以及分布地域过广的基建设备巡检等。

区块链基础设施将有效融合物联网、人工智能等技术，并通过多维度设备管理及巡检数据的打通，提升设备管理及巡检管理效率，收集一线的设备使用情况，从而针对性地改进设备评估方法和提升生产质量。

（二）动态频谱管理与共享

1. 发展现状

在无线通信中，无线频谱资源作为一种稀缺的自然资源，是支撑无线通信数据传输必不可少的重要基石，属于国家重视的重要战略资源。随着通信数据量指数性爆炸式增长，无线频谱资源也面临日益短缺的问题，这是因为传统的频谱规划管理策略为“静态管理策略”，即不同的频段被长期固定的分配授权给频谱拥有者（例如，电信运营商）专用，而适用于无线通信的频段，特别是移动通信广泛应用的低频段（sub 6GHz）频谱资源，也几乎早已分配殆尽，因此，当前无线通信实际上面临着频谱资源严重短缺的问题。

更严峻的是，即使为授权频谱，频谱拥有者也面临频谱利用率低下的问题。例如，在某些用户量较少地区、或者数据量较低的时段，频谱拥有者也不会使用全部的授权频段。一方面，对于频谱拥有者来说，如欧美地区，频谱拥有者为拍卖获得该授权频谱花费了较大的投入，而无法充分利用其频谱获得有效的经济价值；另外一方面，未授权用户也会因为未获得该频段使用授权而无法充分发挥该频段资源的通信价值。

针对上述频谱资源管理与使用效率低下问题，业界也早已提出并使用例如频谱重耕（spectrum refarming）的方法，例如，将2G/3G所分配占用的频谱资源，重新规划给4G使用，或者政府回收部分频谱利用率较低的频段，但是这些方法本质上还是频谱静态管理策略，并

未解决频谱利用效率低下的问题。

为解决该问题，学术界产业界也提出了频谱动态共享的方案，在近期5G及后5G的研究发展中，动态频谱共享更是一度成为各方争相研究的热点技术之一，例如，作为动态频谱共享中的一种认知无线电等技术，可通过对周围环境的频谱动态感知，实现频谱共享、提升频谱利用率的目的。此外，对于动态频谱共享而言，在面临“授权频谱”、“共享频谱”、“免授权频谱”共存的现状，使能三者之间的动态频谱共享还可将无线通信扩展到更多、更广的维度，例如4G/5G蜂窝系统、IOT等物联网垂直行业频谱、wifi等免授权频谱之间的动态共享，更是可以实现各方受益的双赢局面。

虽然动态频谱共享有着上述显著优点，但其技术实现诸多问题，例如 “授权频谱”之间的相互共享、频谱拥有者之间的相互信任、频谱价值转移、资源共享等，都亟待解决。

针对上述动态频谱共享所面临的问题，考虑到区块链由于其分布式记账的本质，且区块链上层智能合约具有使能智能结算、价值转移、资源共享的天然优势，因此区块链很适合与动态频谱共享相结合，美国FCC官员在展望未来6G时，更是表示，随着未来网络的密集化，基于区块链的动态频谱共享将成为未来6G的发展趋势。利用区块链所有参与方都可对信息进行监督，记录不可篡改删除的特点，使得无线频谱资源的共享、价值转移流通过程更加公开透明和真实可信，进而实现不同频谱拥有者无线频谱资源价值变现化、价值转移化和频谱共享化。

2. 解决方案

对于基于区块链的频谱资源共享，对~~以~~拥有“授权频谱”的拥有者而言，可将不同频谱拥有者所拥有的频谱通过区块链记录管理，并在区块链上层部署用于动态频谱共享与结算的智能合约，合约上链公平透明，每个频谱拥有者可作为一个区块链节点，智能合约代码根据预设条件自动执行，内容不可篡改，如图5所示。其中，智能合约的内容可根据频谱拥有者，结合自身频谱使用特点，空闲时段等，确定动态频谱共享机制、进行结算计费等。

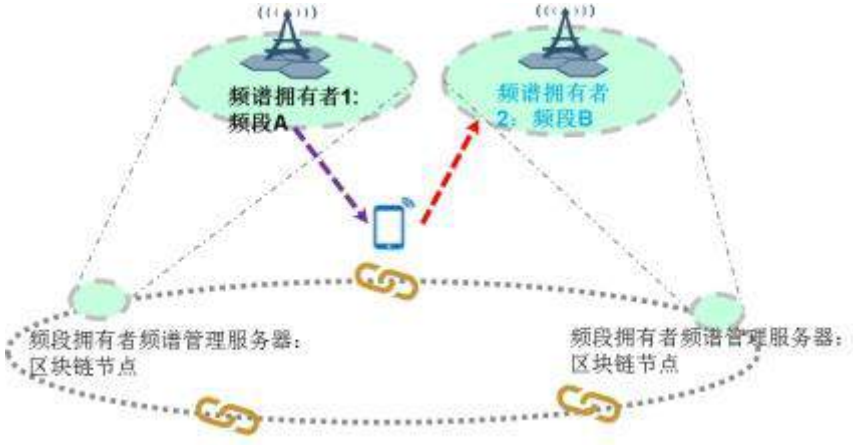


图5 基于区块链的频谱共享方案

在本方案中，频段拥有者的频谱管理服务器可独立部署，也可以基于当前的移动网络进行部署，举例来说，区块链的逻辑功能可以部署在移动边缘计算（MEC，Mobile Edge Computing）网关。移动边缘计算的基本思想是将云计算从移动核心网内部迁移到接入网边缘，实现计算及存储资源的弹性利用。考虑到基于区块链的网络边缘计算具有改善用户体验、节省带宽资源、计算储存能力下沉至边缘节点的优点，将动态频谱共享的区块链功能部署于移动边缘计算的网络实体，

可进一步降低分布式节点区块链部署成本，实现动态频谱共享。

具体的，以一个用户为例，可通过下面一种可能的方案实现动态频谱共享与结算：

1) 用户设备以传统身份认证机制接入使用频谱拥有者1的授权频段A；

2) 频谱拥有者1认证该用户后，授权该用户使用频段A，并为该用户分配用于区块链认证的公钥和私钥；

3) 频谱拥有者1将该用户私钥以加密的方式通知用户；同时将该用户的公钥写入区块链；

4) 用户通过私钥请求使用频谱拥有者2的授权频段B；

5) 频谱拥有者2通过查询区块链上的公钥，确认该用户的合法身份，并在授权该用户使用频段B；

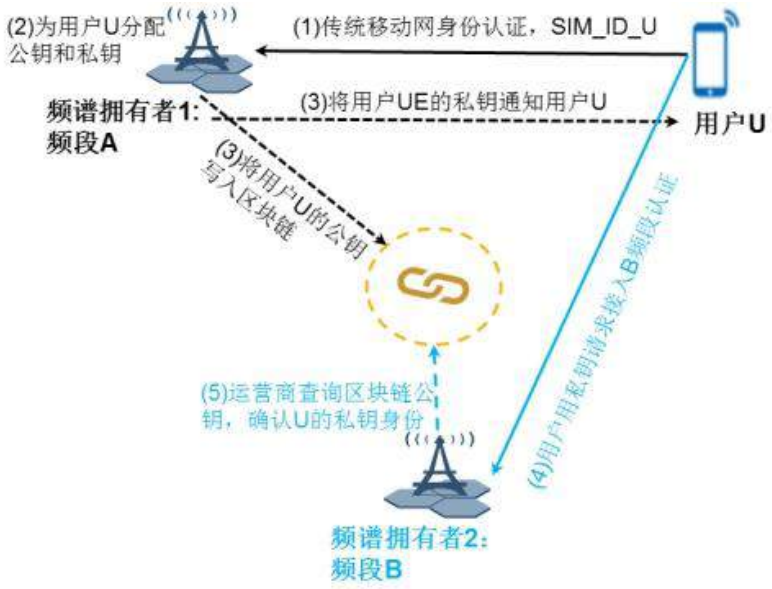


图6 基于区块链的频谱共享方案

在上述方案中，频段拥有者之间可通过区块链动态共享使用各自

所拥有的授权频段，同时还可根据区块链的智能合约，智能的结算租让或者租用另外一方的授权频段的费用，从而既动态提高频谱的利用率，又充分利用空闲频段变现经济价值。

3．发展策略

利用区块链技术使能动态频谱共享，目前尚无此类应用案例。但该方案可提供更灵活、更深度动态的频谱共享，有效的解决了频谱静态管理策略造成的频谱资源浪费问题；同时结合区块链分布式账本及智能合约的天然优势，该方案还有效的解决了动态频谱共享结算和价值转移的问题。对于后续的发展，建议如下：

1）明确应用场景：

明确动态频谱共享的适用范围，结合频谱法律法规，确定可以部署基于区块链动态频谱共享的对象、适用频段等。

2）明确区块链部署：

区块链的部署建议结合网络边缘计算MEC网关，部署在MEC网关实体上，从而充分发挥区块链与边缘计算的双重优势，获取更大收益。

（三）数字身份认证

1．发展现状

身份是一组用于定义某项实体的特征数据，并具有相对唯一性。数字身份是特定实体物理身份的数字版本，个人、资产以及设备等实体都可以具有数字身份。

数字身份认证也称为“身份验证”，是指在计算机网络中确认操作者身份的过程，从而确定其是否有对某种资源访问和使用的权限。

1.1 基于个人的数字身份认证

传统的针对个人进行数字身份认证方式主要有静态密码、动态密码、数字签名、生物识别等。互联网的飞速发展促进了个人身份的多样化，从而使人们可以在网上使用不同的属性或数据来构建一个不同的“身份”，这也为数字身份认证管理带来了极大的挑战。

调查显示，4/5 的人不喜欢网页注册的繁琐过程，35%的在线购物者因为没有账户放弃了他们的购物车。ITProPortal 估计，截止到 2020 年，我们将拥有超过 200 个数字账户。现阶段，我们每个人都有很多个账号，登录各种各样的网站，注册各种各样的 app。随之而来的就是用户隐私被无限的扩散，每天接到各种各样的骚扰电话，更有甚者因为用户隐私泄露而导致财产损失。

对此情况，现有的技术主要是通过社交媒体来进行登录，利用第三方授权机制，采用 OAuth 2.0 协议来完成。OAuth 2.0 协议关注客户端开发者的简易性，要么通过组织在资源拥有者和 HTTP 服务商之间的被批准的交互动作代表用户，要么允许第三方应用代表用户获得访问的权限。像我们常用的微信、支付宝登录都是采用 OAuth 2.0 协议完成的。

利用社交媒体账户登录可省去用户注册的一系列流程，已经成为替代在线注册的主流选择。该方案虽然有很多优势，但也存在不少弊端，例如在安全性上面存在一定的漏洞。2016 年 11 月，香港中文大

学的三名研究人员发表文章称，“使用 OAuth 2.0 协议可以毫不费力地登录十亿移动 LApp 账户”。研究人员发现通过第三方 app 开发方，错误地使用 OAuth 2.0 协议，能在用户不知情的情况下，被黑客远程利用。

针对这一系列问题，区块链技术能够提供一种新的思路，通过多方参与的分布式账本技术，可实现运营商之间的合作机制；通过密码学原理的非对称加密、智能合约以及零知识证明的方式，保护个人隐私数据不被泄露盗取；通过将数据使用的决策权归还给用户，解决用户身份数据使用的合法合规性问题。同时，结合运营商天然具备的大量实名用户信息，基于运营商提供的手机号码和个人信息进行身份验证，可以为用户提供便捷、安全的身份认证服务。

1.2 基于设备的数字身份认证

为适应 5G 和物联网技术的发展、响应国家“互联网+战略，运营商必将面临全新的产业生态环境。一方面，运营商内部网络与业务系统优化、不同系统之间需整合和优化，不同运营商之间互通合作更加密切（如：切片联盟）；另一方面，运营商面对更加众多的产业合作方，必须通过技术手段加强安全的互信合作。PKI 公钥基础设施是一种建立互信的重要技术手段，是运营商对内优化流程、对外协作的安全方案平台，普遍应用于互联网，随着网络与通信技术的发展，在移动通信网、物联网、车联网等场景中的应用越来越多。而它在使用便捷性和互联互通等方面产生了一些新的问题。区块链技术去中心、防篡改、多方维护等特点可帮助 PKI 体系更加透明可信、广泛参与、优

化流程等。

现有证书管理系统存在的问题如下：

1)单点失败问题

CA 是 PKI 技术中的中心信任点，一旦由于 CA 机构自身原因或遭受安全攻击等原因造成服务不可用，将影响使用相应 CA 机构数字证书的用户。

2)证书批量配置效率低

用户在配置和使用证书时，需要首先向 CA 机构申请证书，CA 机构签发证书后，用户需要将签发的证书配置或安装至目标设备中。在移动通信网、物联网、车联网等场景中，由于涉及数量巨大的网络设备和终端设备，批量配置私钥和证书的需求极为迫切。

以 LTE 小基站为例，该设备需要配置数字证书实现设备认证。由于需要为每台设备配置不同的私钥和证书，难以实现批量操作，不仅施工效率低，还存在因为人工操作导致私钥泄露的安全风险。

3)多 CA 互信难

用户证书只能由所属 CA 的根证书进行验证，不同 CA 之间不能相互验证。该问题目前有权威 CA 列表、CA 交叉认证、桥 CA 等解决方案，但权威 CA 列表更新和维护代价高，CA 交叉认证不适用 CA 数量较多的场景，桥 CA 技术存在运营方选择的问题，每种解决方案都存在一定的局限。

利用区块链去中心化、不可篡改等特性，在区块链上构建 PKI 数字证书系统，该系统继承了区块链自身固有特点，相对于对传统 PKI

技术具备多方面的技术优势：

- 去中心化解决单点失败问题

基于区块链的 PKI 数字证书系统由若干验证节点、证书用户、以及依赖方共同组成区块链网络，无中心节点。一个或多个节点出现故障或遭受攻击均不影响整个系统的运行。

- 降低 PKI 技术使用门槛

企业或个人在使用 PKI 技术时，无需向第三方 CA 申请证书，也无需单独部署 CA 系统，加入该区块链 PKI 数字证书系统，即可使用该系统提供的证书服务。可有效节约向第三方 CA 申请证书的费用，解决建设、维护、以及运行 CA 系统所需的费用。

- 提升 PKI 技术使用体验

系统改变了证书签发与配置逻辑，即，由传统的“CA 签发证书、设备配置证书”改变为“设备签发并配置证书、区块链 PKI 系统发布证书”，将传统方案中的证书申请与获取的交互过程，改变为证书单向提交的过程，有利于设备在生产线批量生成和配置证书，提高证书配置效率。

2. 解决方案

2.1 基于个人的数字身份认证

运营商具备大量的实名认证用户，可以利用算法为每个用户建立唯一的数字身份，使用该数字身份通过验证后可以代替所有的数字账号，结合区块链技术来确保数字身份不被篡改，用来进行各种认证。

当用户使用运营商的应用打开一个帐户时，运营商利用算法为用户创建数字身份。与此身份相关联的私钥安全地存储在各自用户的 eSIM 上，公钥存储在所有节点上。然后它使用自己的私钥添加数字签名，数字签名等摘要信息上链用来进行验证。示例图如图 7：

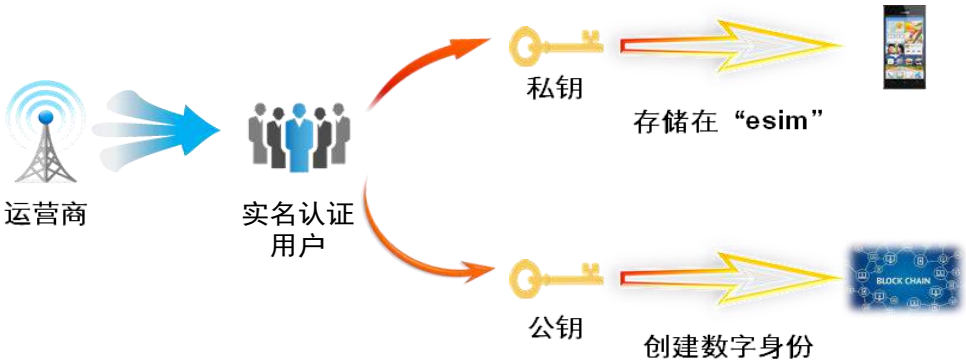


图7 数字身份创建过程

用户统一身份认证，所有运营商用户数据信息生成摘要（公钥，数字签名等）放在链上，其他的 APP 需要身份认证的时候访问链进行认证，对于其他 APP 来说，用户是匿名登录，保护了用户隐私，避免了用户信息泄露。

第三方开启授权认证时可以通过授权平台对授权信息进行查询，通过智能合约技术实现对数据信息的查询，通过链完成验签过程，第三方从链上直接获取认证结果。

具体流程图见图 8：

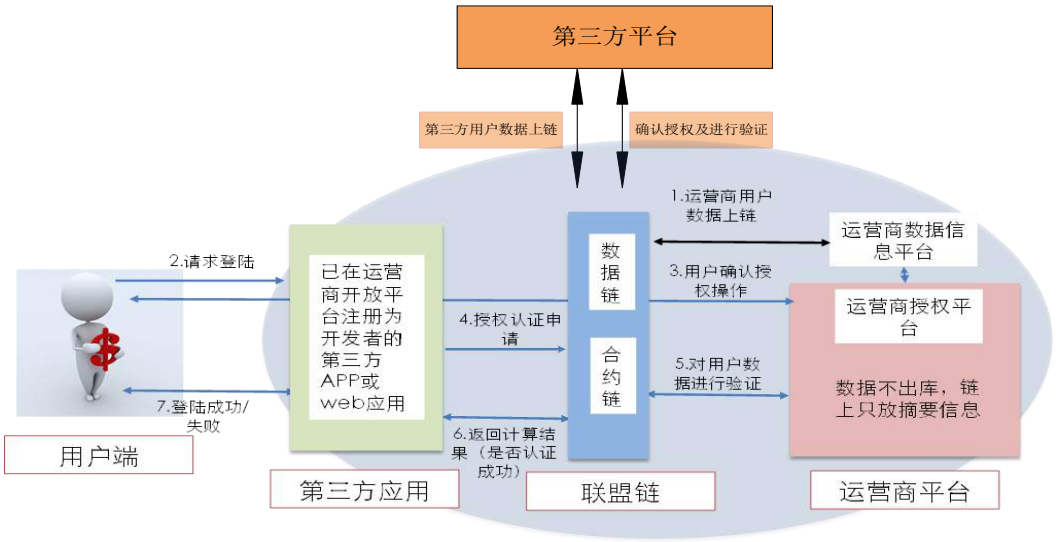


图8 数字身份认证过程

1) 运营商将自有实名认证的用户数据库，通过算法进行加密，可以生成公钥和私钥对，利用私钥生成数字签名。其中，公钥和数字签名上链进行存储。私钥存储在用户本地，即 eSIM 卡上。

2) 用户请求登录在运营商开放平台注册过的第三方 APP 或者 web 应用。

3) 第三方 APP 或者 web 应用将用户请求信息发送给运营商授权平台，授权平台提示用户，获取用户授权登录信息，在此基础上提示用户信息使用范围，是否允许第三方使用用户信息（该步骤不影响用户后续登录操作）。

4) 第三方 APP 或者 web 应用获取用户授权之后，开始上链进行验证申请。

5) 第三方 APP 利用用户提供的信息，在链上匹配公钥和数字签名，同时在运营商数据库内部进行匹配。

6) 将匹配结果反馈给第三方 APP 或者 web 应用

7）根据反馈的结果对用户的登录请求进行回应，匹配成功则登录成功，否则就登录失败。

8）只要加入联盟链中的企业都是可以共享认证用户，假设第三方企业也有自己的认证用户数据库，则这些用户可以直接登录联盟链中的其他应用，原理和流程同上述方式。不同企业之间可以在保护自己用户数据的前提下共享彼此的用户，达成统一的认证。

用户通过本方案创建的数字身份，在条件允许的情况下，可以用来代替其他所有的数字账号，同时也对于安全性和可控性方面有了较大的提升。并且该数字身份不仅可以用来进行第三方合作伙伴验证，还可以用于社会中需要实名注册的地方，比如车站、门禁、银行等等，在保护用户隐私的同时，极大的方便了用户，同时监管层也可以定位到具体用户。

图9 数字身份扩展应用

2.2 基于设备的数字身份认证

基于区块链的 PKI 数字证书管理系统的目标是利用区块链技术

提升传统 PKI 技术的易用性，扩展 PKI 技术的应用场景。该系统利用区块链去中心化信任的特点，在设备商、运营商之间建立信任关系，将传统 PKI 技术集中式的证书申请、状态查询改变为分布式实现。利用该系统，设备可自行生成并提交证书，区块链节点使用智能合约验证和写入证书；证书使用过程中，依赖方通过区块链检查证书的正确性和有效性。

在区块链技术中，一旦数据通过共识之后记录到区块链中，那么数据就被所有参与方认可。因此，将通过共识的数字证书记录到区块链中，就可以使这些数字证书被所有参与方认可。区块链没有中心化的信任节点，区块链数据也以分布式的方式存储于多个节点之中，破坏任意节点均不会导致区块链数据丢失，因此，在区块链基础上构建 PKI 数字证书管理系统，可以解决传统 PKI 技术的单点失败问题。

由于区块链没有中心化信任节点，因此可以实现证书用户自行生成证书，区块链节点按照规则判断证书是否真实有效，如果真实有效才可发布到区块链当中，这样可以解决传统 PKI 系统中先申请证书再配置证书的应用逻辑，改变为先产生配置证书再发布证书，可有效提升证书批量配置的效率。

如果参与共识的节点仅限于 CA 机构，那么就在多个 CA 机构之间建立起信任关系，可以解决多 CA 互信难的问题。

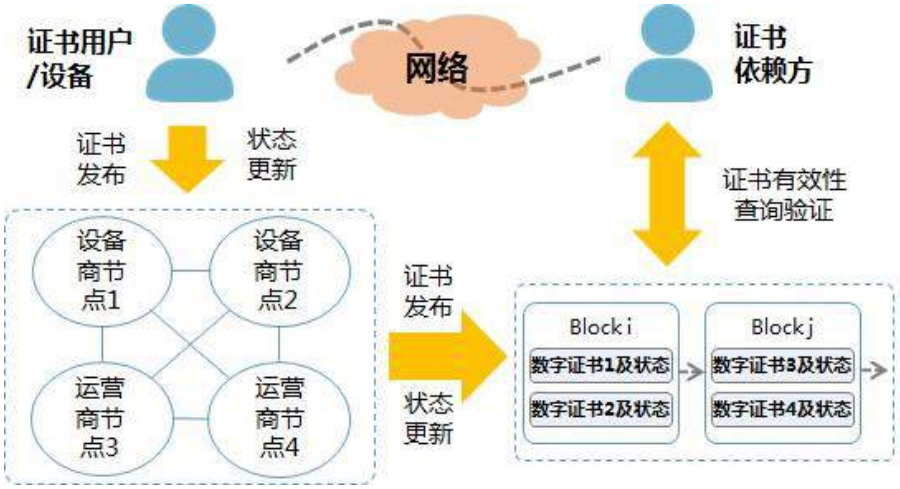


图10 基于区块链的身份认证

3. 发展策略

通信运营商可基于自身的海量数据实名信息和手机号码的关联关系，打造基于区块链技术的身份认证平台，可以提供诸如统一身份认证、身份信息校验、免密登录等服务。

1）采用区块链建立跨运营商的移动用户身份认证平台，提供具有电信属性（包括手机号码、IP 地址、SIM 卡属性、手机号码使用权等）的身份认证服务，免去短信验证码的交互，降低隐私泄露和安全风险；

2）基于区块链技术创建一种可以共享身份验证信息及结果的分布式节点网络，联合电信运营商、互联网公司、银行等对用户认证数据有需求的企业，形成统一认证联盟。

3）以手机号码、姓名、身份证号、性别等实名信息为基础，通过区块链技术搭建手机用户、电信、数据应用方之间的桥梁，实现数据的高效共享，在用户授权的前提下，将用户身份信息提供给数据需求方，建立合法、合规、便捷的身份认证平台。

4）通过多方参与构建的身份信息联盟链，以手机号码为标识，结合基于哈希算法的隐私保护技术，通过自动执行的智能合约，识别身份信息的不一致冲突，为运营商或其他需求方作为参考，以甄别欺诈用户，提供黑名单预警。

此外，基于区块链的 PKI 系统可为多种场景提供高效便捷的数字证书服务，在家庭网关、小基站、安全芯片、智能硬件等领域有着广阔的应用前景。应用场景有：

1）小基站接入认证系统：小基站是一种小型化、低功率蜂窝技术，通过固网宽带接入到移动核心网，是室内覆盖增强方案之一。小基站与安全网关之间采用数字证书方式进行双向认证，之间建立 IPsec 通道确保传输安全。数字证书能有效保护设备及通信安全，但设备从制造到入网涉及 OEM 厂商、设备商、销售商、运营商、用户等多角色，由于信任、效率问题在批量制造或部署环节灌注证书面临较大挑战，利用基于区块链的 PKI 数字证书管理系统，将设备商、运营商作为区块链的节点，使用联盟链实现小基站证书的分布式发布和管理 。应用场景如下图 11 所示：

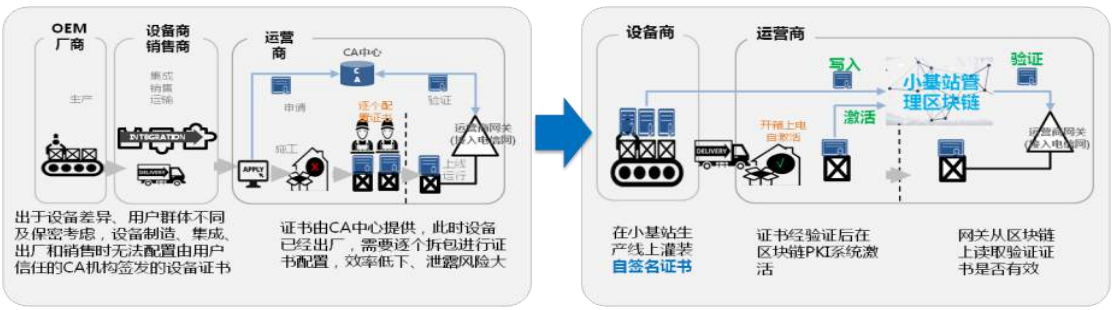


图11 基于区块链的PKI数字证书管理系统

2)切片互信:切片是 5G 的重要特性之一,针对不同业务场景(MBB、

海量物联网等）的需求，以切片形式为 UE 提供网络功能和配置的集合，使得运营商能够基于垂直行业的需求创建定制化的专用网络。端到端的网络服务可能需要位于多个国家多个运营商的切片进行互联，共同提供无缝的跨国家域、跨业务的 5G 业务。

切片间通信需要进行安全保护，安全信道的建立可采用数字证书技术实现，但不同运营商的切片通常使用不同 CA 签发的证书，在建立 CA 互信之前，无法实现相互认证。

图 12 是多个切片互联场景中使用上述联盟链进行认证的示意图，配合切片间连接的弹性变化，可以方便地建立不同 CA 间的互信，从而支持跨运营商切片业务灵活、安全、快速开展。

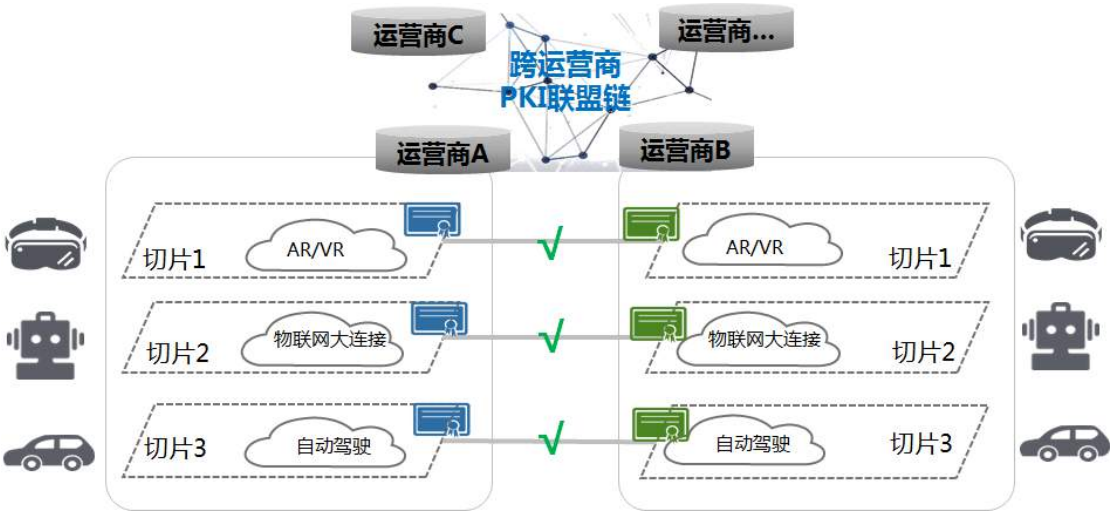


图12基于联盟链的认证

3）异厂家物联设备安全直连及管理：在多厂家设备混合组网的环境下，不同品牌设备有不同的证书链，无法建立安全通信通道，无法统一管理，比如家庭智能设备间的互联。 使用区块链实现跨厂商的证书联盟链，便于不同 CA 签发证书间的互信，从而实现设备间的安全通信和设备的统一管理，利于设备的智能互联。

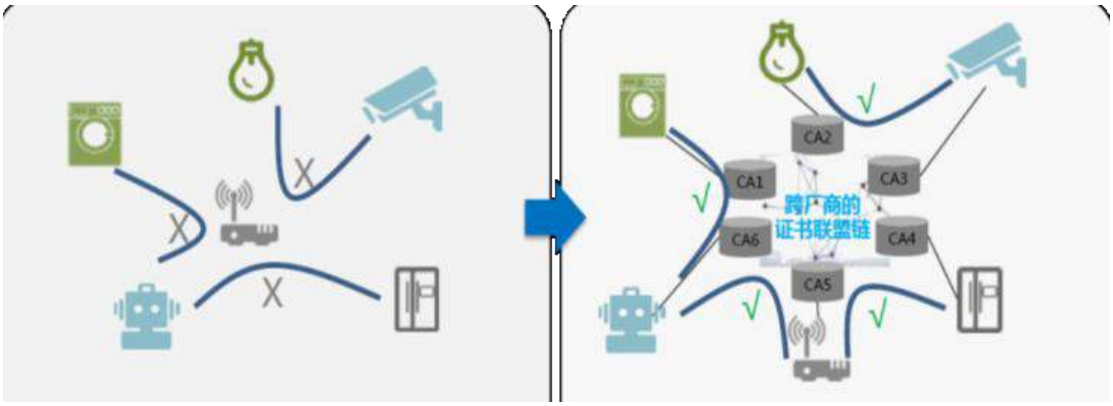


图13 跨厂商的证书联盟链

（四）国际漫游结算

1. 发展现状

从国际漫游结算机制来看，国际漫游资费的产生过程较为复杂，国际漫游资费的形成是由归属国运营商用户到漫游国发生境外通信后，由漫游国运营商对漫游用户提供通信服务并进行漫游计费，再将漫游计费数据传回归属国运营商，由归属国运营商对漫游用户进行收费，同时跟漫游国运营商按照约定的资费进行漫游批发结算。目前，全球有 700 多家运营商，若开通漫游业务，都需要彼此之间进行相互的漫游关系的建立，漫游协议的谈判和漫游结算等相关工作。

GSMA 组织根据国际漫游业务开展过程中运营商需要获取的信息，制定出标准的文档格式，形成了标准国际漫游协议文档。国际漫游协议是用于国际漫游运营商间制作对方局数据的重要规范文件，运营商可以通过文档的交互和解析获得漫游业务结算相关信息，开展漫游业务日常运营。常用的国际漫游标准协议主要包括两类：AA.14 和 IR.21。AA.14 协议主要包括标准资费（IOT）信息和运营商联系（OPDATA）

信息， IOT 文档包含了漫游地运营商的标准漫游资费，OPDATA 文档包含了漫游地运营商的商务联系信息，财务清算信息，服务和安全信息等。国际漫游 IR21 文件包含了路由，SCCP 网关，自动漫游测试，移动应用，GPRS 等网络层配置和管理信息。一般的漫游及清结算过程如下图 14 所示。

图 14 一般的漫游及清结算过程

虽然有 GSMA 定义的相关规范和标准，但运营商之间的漫游关系是一个相对松散的联盟关系，目前在国际漫游结算方面，依然存在着很多问题：

1）从争端处理机制来看，一般漫游结算中出了问题一般需要运营商之间层层升级，一直到国际组织去仲裁，同时由于是跨国处理，需要耗费很大的协调成本和时间成本。

2）从漫游协议文件和财务结算文件的传输方式来看，目前运营商仍在通过人工发送 e-mail 的方式传送文件，其可靠性差，受人工干预的影响较大，相关文件的延迟接收和维护将延迟国际漫游结算的及时性。

3）从处理时效性来看，运营商传输协议时，因为发送的漫游伙伴较多，可能导致人为的分发错误，同时由于运营商网络连接方式的多样性，传输可靠性易出差错。对于漫游资费这类有时间生效要求的文档，如果运营商未及时巡检接收协议，可能导致计费/财务/欺诈等关键信息配置不及时，导致生产事故，使运营商遭受巨大损失。

4）从漫游管理模式来看，目前协议管理都为单边管理方式，无

法完全保障双方协议的一致性，运营商无法对漫游协议进行统一管理。如果运营商间对协议内容发生分歧，无法追溯查找问题发生原因，容易造成争议。虽然在运营商之间出现了漫游清算中心，相对可以简化运营商之间漫游清结算的多边处理关系，但从清算中心的职能来看，更多的是运营商的代理人角色，作为专业化运营机构减轻运营商的漫游处理工作，而无法承担起运营商之间作为公证中介的角色。

2. 解决方案

利用区块链系统可信高和防篡改的特性，运营商及其漫游伙伴之间可以共享一套可信、互认的漫游协议文件及财务结算文件体系，所有的漫游公参记录全部都上链，实现可查可追溯，安全透明，提升结算工作效率，减少之前因不一致带来的复杂的争端处理和仲裁机制。如下图 15 所示。

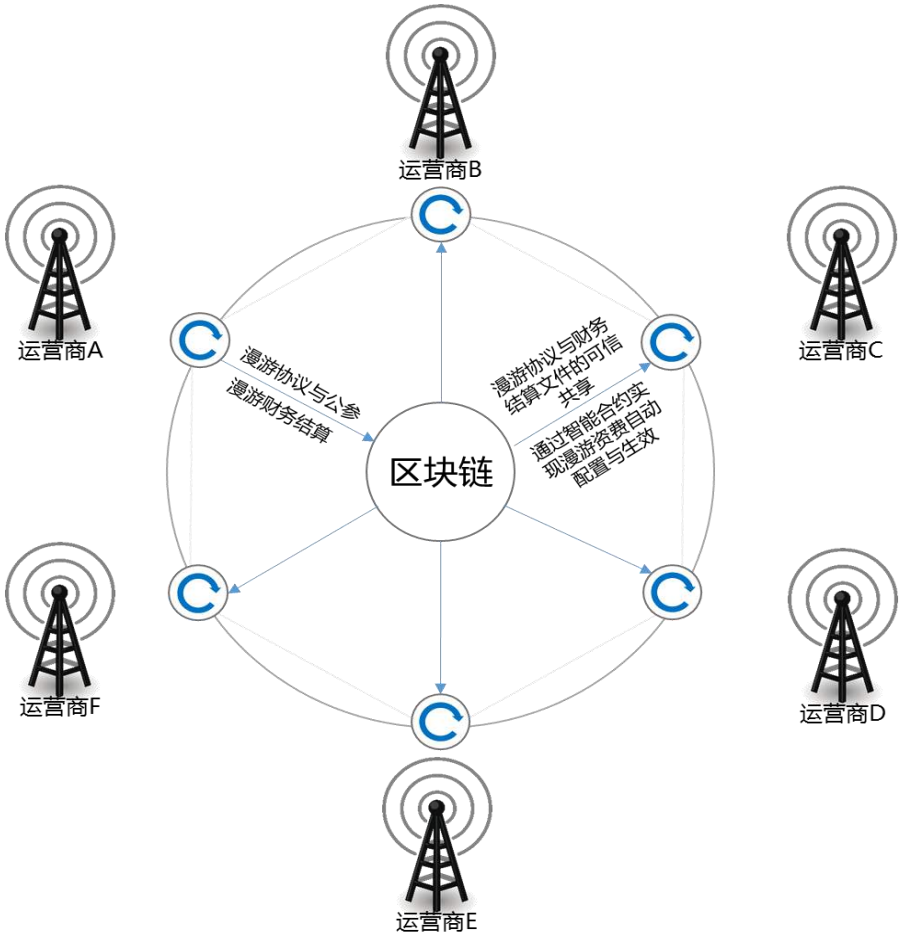


图 15 基于区块链的漫游管理模式

此外，区块链适合用于有时间戳要求的场景，如漫游协议资费和公参的生效管理，漫游财务结算文件的传递和状态变更需求等。通过搭载智能合约，可以实现自动执行漫游公参更新的自动化配置，从而实现漫游协议发布配置生效一条龙管理，进一步降低运营人员成本和差错率。

使用区块链系统，可大大减少各运营商传统的进行协议文件巡检和处理的人工工作量，以及和跟海外运营商进行申告处理的时间，降低双方的人力成本；同时，提高了协议文件的传输可靠性，确保了漫游结算资费的准确性；有利减小财务审计如计提和应收应付账款的风险压力。

3．发展策略

目前将区块链系统用于国际漫游结算的漫游协议管理及财务结算中，并在我国运营商漫游业务较为密集的亚太等运营商之间进行场景验证和试用推广，利用实际应用效果，逐步向漫游伙伴推广经验，建立信任机制，引导国际运营商和国际漫游清算中心认识到区块链技术对于国际漫游清算行业的重要意义，完善区块链技术在漫游业务的应用环境。

下一步，与国际标准组织 GSMA，3GPP 等展开合作，推进和细化各类漫游协议的标准制定和实施，加强区块链技术与国漫清算业务的融合范围。继续开展实现协议/账单/话单等全业务数据的上链传输与链下运营商系统数据自动交互和解析处理的研究，最终完成基于区块链技术的漫游清算全业务处理，从而极大的提升国际漫游自动化清算的效率。

（五）数据流通及共享

1．发展现状

随着大数据的广泛普及和应用，数据资源的价值逐步得到重视和认可，数据流通和共享的需求也在不断增加。数据的流通和共享有利于最大化地挖掘出数据资源的潜在价值，推动产业模式创新和产业转型升级。早在 2015 年，国务院《促进大数据发展行动纲要》中明确提出“鼓励产业链各环节的市场主体进行数据交换和交易，促进数据资源流通，建立健全数据资源交易机制和定价机制，规范交易行为等

一系列健全市场发展机制的思路与举措”。电信大数据，因其真实、完整、规范、质量高、应用广泛等特点，数据流通和共享的需求也更为紧迫和强烈。

当前在国家政策的积极推动、地方政府和产业界的带动下，很多地方和企业等率先进行了大数据流通和共享的探索，比如北京、贵阳、江苏、上海、浙江等地的大数据交易中心。三家电信运营企业目前都在积极开展各类对内大数据应用支撑和对外行业变现，也都对电信数据的流通和共享进行了积极布局和实践。但总体而言，电信大数据数据流通和共享目前还处于起步阶段，大部分数据仍集中在三大运营商内部，尚未形成在多行业、多数据所有方、多数据应用方之间的数据流通畅通通道，电信大数据在社会管理和经济发展中还未发挥充分作用，造成大量数据价值的流失。

目前，电信大数据的流通和共享存在着如下三个主要问题：

1）数据交易整体大环境的规范性和完备性不足，交易过程中的数据确权、数据定价等核心问题尚未得到全面解决。因我国的大数据流通市场的初级性，相关法规、行业公约、规章制度和保障体系等都处于初期阶段，权益体系与监管体系不完善、分级分类机制缺失，虽然各交易平台建设过程中自行探索了标准体系，出台了各类公约，但自成体系，对大数据流通交易中的很多共性敏感问题，如数据定价、数据确权等，并没有全面、权威、有公信力的解决方案。

2）数据安全和隐私保护的要求愈加突出，随着《中华人民共和国网络安全法》的正式实施，贩卖非法数据正式入刑。但由于整体数

据流通体系各环节缺乏统一共识，如第一点所说的很多问题没有准确界定等，电信企业为了规避风险，往往在数据共享和交易中采取非常谨慎的策略，在某种程度上增加了数据流通的难度，缩小了数据流通产业规模。因此，数据流通领域亟须通过新的技术应用，帮助流通环节中的各个企业建立足够的数据安全体系保障。

3）现有的数据流通方式以“中心化”方式为主，如政府机构参与构建的集中数据共享的方式，或者一家汇聚数据提供方和数据需求方的数据交易中介机构，或以数据生产或数据服务类企业为主导、商业职能为主的数据交易平台。这种“中心化”的模式较为适合政府集中管制的行业，如银行业等；或者行业内有一家具有广泛公信力的中介机构存在。而在电信领域，非政府强管制；且电信大数据被三家运营商分别拥有，并不存在一家广泛公信力的中介机构；三家运营商由于各自用户群不同，以各自企业为中心的平台也只能提供部分数据，且不利于跨行业的数据融合共享。

2. 解决方案

分析数据流通领域的现状和问题，在电信数据流通共享的流程中，区块链可以在以下几个领域提供较为合适的技术手段。

2.1 构建“去中心化”数据流通和共享生态体系

区块链所具有的分布式、自组织特性，可用于构建数据共享、分散协作的去中心松散生态环境。电信数据主要来源于三大运营企业，其数据类型、格式和内容存在很大程度的相似性，很容易应用于同一需求场景。三大运营商或其数据代理机构、或持有电信数据的中介方、

数据需求方等可根据情况自愿组成联盟链，数据持有方将能够共享的数据元信息、样例数据等在链上进行公开，需求方可根据自身需求提出数据获取需求，达成的数据交易及数据权属流转信息的转移也都记录在链上。以区块链技术为基础，构建“去中心化”的新数据流通体系。

依靠区块链提供的分布式账本结构，让数据交易流通记录能够做到公开透明、不可篡改和可追溯，充分反映流通各环节状况，建立数据流通各链条之间的信任关系。

基于共识机制，在数据资源产生或流通之前，将确权信息和数据资源有效绑定并登记存储，使全网节点可同时验证确权信息的有效性，并以此明确数据资产的权利所属人。通过数据确权建立全新的、可信赖的大数据权益体系，为数据交易、公共数据开放、个人数据保护提供技术支撑，同时为维护数据主权提供有力保障。

基于区块链技术，可以依据智能合约等对流通的数据进行统一的分级分类管理，从而进行统一定价，解决价格不统一、随意定价等问题。

在数据安全保护方面，依托智能合约独立运行的沙箱环境，除了数据授权方和利益相关方，无人能够接触到相关数据，并且严格按照智能合约设置的数据查看权限进行数据访问，这从一定程度上保证了数据的隐私性。

同时，在数据交易中，通过建立规则，并用智能合约代码表述形式代替合同，实现链上支付、数据访问权限自动获取等功能，提高交

易的自动化水平。

2.1.1 业务角色及功能

图 16 业务功能用例图

a.数据管理员—数据发布

数据管理员负责发布其部所在方的脱敏数据，由各参与方指派专人完成，数据管理员通过管理界面将脱敏数据导入，执行智能合约存于链下数据库同时完成数据上链操作。有条件的参与方可直接开放数据库给区块链系统，通过智能合约直接与脱敏数据库对接，实现脱敏业务数据的实时同步。无论哪种情况，最终通过业务系统脱敏后的数据与区块链基础平台之间的相关接口上链统一管理。

b.数据查询人员—数据查询

数据查询人员可为各参与方共同选举出的行业监管人员、各参与方工作人员、企业法人代表、用户等人群，可通过多种渠道进行信用的查询。所有渠道查询请求均通过接口层，传递到区块链基础平台完成对特定的信用主体的数据进行提取。

2.2.2 技术方案

基于区块链的可信数据共享系统，信用服务中心要与各参与方相

联，为防止网络节点数多、网络规模较大，影响系统性能，共享系统采用小规模多维链的架构，如图 17 所示。

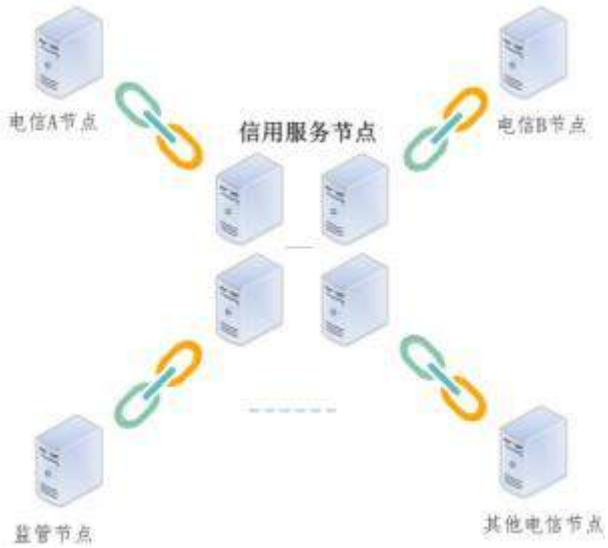


图 17 数据共享多维区块链架构图

图 17 的每维子链仅由一个参与方节点、一个监管节点、一个信用服务平台节点组成，网络规模小，消息传播速度快，可满足系统高性能的需求；同时又可发挥区块链数据存储安全一致、受信任、可追溯、不可篡改的基本特色。

单维子链的体系架构如图 18 所示，区块链作为底层基础设施，通过接口层的链下共享数据库及智能合约将信用服务中心与参与方各业务系统进行共享链接。查询数据通过信用服务中心业务系统进行查询的相关数据。

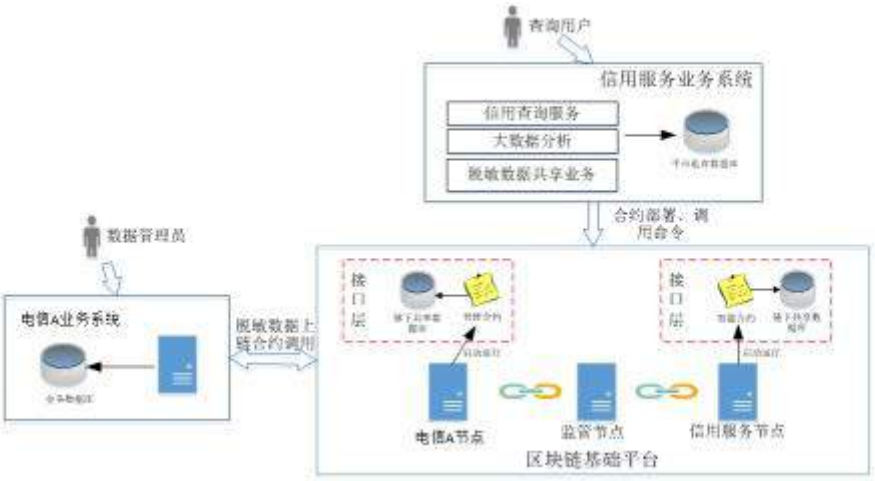


图 18 单区块链总体架构示意图

体系架构分为三层，从左到右依次为：业务系统、接口层、区块链基础平台。

a. 业务系统

业务系统包括各方自有的用户界面及特定的业务功能，也包括与底层区块链基础平台相关的数据发布、查询等功能。各业务系统可完成脱敏数据的上链、在链上被其他节点所查询等操作。业务系统通过触发接口层的智能合约调用，与区块链基础平台交互。

b. 接口层

接口层包含链下共享数据库和智能合约。链下共享数据库存放链上 hash 值对应的明文数据，包含脱敏数据的原始信息、变更信息等。为满足操作可追溯功能，链下数据库以数据（脱敏数据记录均有唯一编号记录）为中心进行设计。

智能合约完成业务相关的验证或其他自动执行的事务，根据业务需求进行代码编写，如脱敏数据发布、脱敏数据查询等。智能合约操

作链下数据库，并将对应的 hash 值上链。

c. 区块链基础平台

区块链基础平台由多个节点的 P2P 网络组成，提供合约部署、调用、hash 值上链等 API 接口。接收到智能合约调用命令后，平台将采用虚拟化技术启动、运行合约代码，响应 hash 值上链操作，以及对 hash 值达到共识后存储。

2.2.3 业务系统改造

各业务系统与区块链基础平台进行交互时，需要针对原有系统进行一定的改造，以实现触发对区块链平台上智能合约的调用。改造主要涉及到以下四个部分，如图 19 所示。

a. 脱敏数据上链

各参与方的业务系统生成脱敏数据后，需按区块链基础平台要求封装智能合约的调用接口数据，触发“数据发布”智能合约调用，进行脱敏数据上链操作。调用接口可以是业务系统直接调用，也可以是通过用户操作界面将脱敏数据包导入后调用。

b. 数据查询

可信数据共享系统可通过区块链提供的“数据查询”智能合约查询信用主体的在各参与方共享的数据信息，为了能确保数据的实时更新，可仅查询各节点的链下数据库系统，再返回显示给用户。

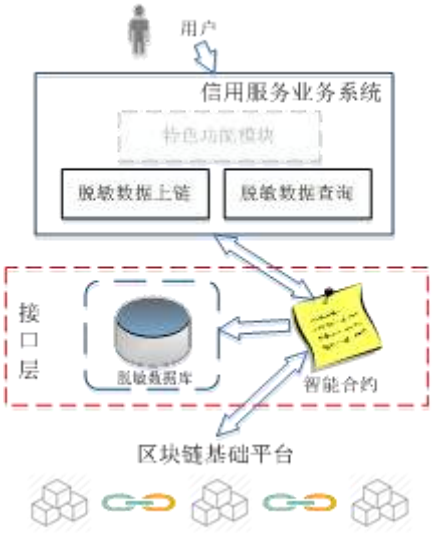


图 19 信用服务业务系统与区块链平台关系

c. 接口层设计

在各业务系统的使用过程中，图 19 中底层的区块链基础平台并不直接与终端用户交互消息，而是通过接口层，以智能合约的形式接收业务系统发送的合约命令及参数。智能合约事先被部署在区块链基础平台上，平台接收到业务系统发送的命令后，启动及运行相应的智能合约代码。智能合约进行业务数据操作相关的验证工作，并将操作结果 hash 值送至区块链基础平台达成共识存储，再更新链下共享数据库。

区块链基础平台在与业务系统对接的过程中，接口层的设计与实现包含了如下两个部分：智能合约和链下共享数据库。

a. 智能合约

区块链基础平台支持图灵完备的智能合约代码，智能合约事先部署到区块链上，返回平台认定的 ID，被调用时提供给业务系统的接口包含如下四个参数：

- chaincodeID:向区块链基础平台指示待启动运行的智能合约 ID;
- businessID：向区块链基础平台指示智能合约中上链数据所属的业务 ID;
- 命令：向待启动运行的智能合约指示将要执行的操;
- 命令参数：为智能合约操作命令提供执行时所需的输入参数。

可信数据共享系统中应设计两类智能合约:脱敏数据上链及脱敏数据查询。

- 脱敏数据上链智能合约

该智能合约验证数据管理人员签名及参与方节点签名，确保上链共享的脱敏数据经过授权、可信且不可抵赖。验签成功后，合约调用区块链平台 API 对号源信息的 hash 值上链共识存储，再将明文存放到链下共享数据库中。

- 脱敏数据查询智能合约

该智能合约根据信用主体的唯一标识检索接口层的该信用主体在各个参与方的共享数据库。

b.链下共享数据库

区块链基础平台的分布式 P2P 网络由三个节点构成，节点逻辑角色分为验证节点和共识节点。为了达到信任，验证节点集合之间需要数据透明共享，这些明文数据存放在验证节点的链下共享数据库中。

2.2 用户隐私数据授权验证体系和安全审计保障

在公开市场进行合法数据交易的数据按法律规定，都不应包含用户隐私信息，因此多为群体统计数据或脱敏明细数据等。但电信数据

的特点决定了其能够在个人真实数据领域发挥更大价值。对于某些应用场景需要获取用户隐私数据，比如小额信贷应用需要获取申请用户上月话费评分和欠费状态等场景，这种情况需要根据用户的授权情况提供涉及用户隐私的数据共享。

当前的应用场景下，请求用户授权的为数据应用方，授权操作在用户和数据应用方之间进行，如要求用户在线签订的授权协议和知情协议等。这样，授权信息主要保存在数据应用方，但提供数据的数据拥有方或数据管理方对这一授权过程并不直接参与和实时知晓，更多的是事前审核协议文本或事后审查签约记录。利用区块链技术，在数据提供方、数据应用方、用户、数据管理和审计方之间建立联盟链体系，将用户对数据应用方的授权信息、相对应的数据提供记录进行上链，供数据使用方在提供数据前进行验证，数据管理方针对数据授权信息和提供信息进行审计核查。更进一步，数据提供方/管理方（电信运营商或监管部门）可实际参与到用户授权确认流程中，如向用户发送短信验证码等，进一步确保用户授权操作的真实性。

隐私数据授权验证体系利用区块链提供的不可篡改和可追溯以及智能合约机制，构建完善的隐私数据共享的安全保障机制。用户的隐私数据授权给哪一方或哪几方、授权范围和内容是什么，授权时间、有效期、流水号、操作验证码等，都可以在链上被有权限的一方查验，且记录不可更改，再结合后续的隐私数据提供记录，可以方便地进行隐私数据共享的监管和审计。

2.3 数据流转溯源

区块链提供的不可篡改的、全历史的分布式数据库，可以应用于电信数据流通溯源。在数据溯源应用中，可以将交易的数据分块打上数字水印，并将每块交易数据的标识、描述、水印、权属等信息写在区块链上，后续数据流转方或使用方将该数据的流转和使用记录也记录在链上。这样，每块数据的交易流转路径都清晰和明确的记录。整个溯源信息由多方互相验证其信息有效性，杜绝了伪造数据，同时又能对数据的流转进行溯源。当用户对数据有疑问时，可以准确方便地回溯历史流转记录，判别其数据来源和真实性。

2.4 提供电信企业内部数据开放共享的审核、监督和管理手段

区块链技术能够对在电信企业内部数据共享过程中的审核、监管、审计等提供有效手段。除了对外的数据交易，电信运营企业内部的业务部门、省分、地市和部门个人也有利用大数据进行业务创新的需求。而企业内部的数据共享的审核监管手段较为粗放和多样，手段也包括线下审批单、线上工单、甚至邮件、会议等方式，在总部和省分、地市各级公司中也不尽相同。按照国家有关法规，电信企业内部需设立信息安全管理部门，信安管理部门也需要对企业内部的数据流转进行监管和审计。可以利用区块链技术，企业内部的数据生产单位、各级数据需求单位、相应的审批管理单位等组成联盟链，将数据需求提出、需求审批流程、数据需求完成等上链，方便管理部门进行查验和对内部数据共享情况进行追溯。

3. 发展策略

对于数据流通和共享领域的区块链四大类应用场景，根据其业务

需求成熟度、需求迫切性、实施难易程度建议采取不同的策略。

在数据交易领域，可由产业联盟等组织牵头，在各交易方之间进行区块链架构的试点，初期可仅将可供交易的数据的元信息和交易信息上链，实现数据权属验证和交易记录审计，后续可根据情况将自动化交易、数据溯源等功能上链。

用户隐私数据授权体系领域，初期可由三大运营商各自进行体系搭建，时机成熟三大运营商可形成共同联盟，甚至吸引其他行业的数据流通方加入，进一步扩大联盟范围。在用户授权的具体流程上，初期可先尝试授权信息的存证，根据业务开展情况实现用户在线授权和在线验证等功能。

数据溯源：数据溯源主要应用在数据交易领域，其业务开展可先由某数据提供方或数据中介自行进行溯源的实践，条件成熟时加入更多数据交易方。

数据共享审核监管：选择在有条件的电信运营企业内部进行试点。

（六）物联网

1．发展现状

物联网作为继个人计算机、互联网之后，当今世界最具发展前景的产业之一，是新一代信息通信技术高度集成和应用的典范，正在强力与经济社会深度融合，深刻改变生产活动、社会管理、公共服务，促进产业结构优化升级，引领战略性新兴产业发展，推动社会生产和经济发展方式的深度变革。随着物联网技术在行业中的普及和不断深

化，人类社会正进入“万物互联”的新时代。

毫无疑问，物联网已然成为当今世界技术创新最活跃、发展空间最广和应用潜力最大的领域之一。伴随着人工智能、边缘计算、区块链等新技术的不断兴起以及相关产业要素的完备，物联网必将进入智能发展的新阶段。

物联网平台现状分析如下：

物联网的分层架构为：智能设备层、网络设施层、支撑层和应用层组。其中，物联网平台作为支撑层重要网元，提供对物联网设备和应用的管理和通信能力，处于产业链核心位置，而其核心功能之一的能力和数据的开放，为物联网数据的价值体现提供了强力支撑。

然而尚有诸多问题制约其发挥潜在能力，包括：

1) 平台接入的设备众多，设备本身及其采集数据的安全与可信难以保证，设备之间亦缺乏有效的数据交换机制；

2) 后台具有集中存储设备和用户的数据、及控制设备的能力，易对用户造成隐私和安全方面的困扰，缺乏有效的信任机制，使得大量数据难以发挥真正作用和价值；

3) 构建在同一或者不同平台上的各类行业应用之间缺乏有效的协作机制，应用数据的价值流转仍为困难。

物联网应用现状分析如下：

目前对于物联网与区块链的融合应用，在单个垂直行业中首先展开，比如食品行业已有相对成熟的溯源应用。在跨行业融合上也有一些案例，比如供应链应用，物联网+金融应用等。整体上来看，可

以看到，物联网已经应用于许多领域且取得了成功，特别是对于智能健康等高附加值的应用。然而物联网仍面临这一些关键的挑战，将区块链与物联网相结合，会给物联网带来新特性：

（1）更高的可信性。物联网需要在诸多设备中建立可信网络，区块链的结合可以为设备本身和设备间的连接带来更高的可信性。

（2）更高的可扩展性。传统的物联网架构是中心化的，新设备的接入成本较高，区块链的去中心化特性可以有效降低接入成本，从而为物联网带来更高的扩展性。

（3）更灵活的权限控制。区块链的权限管理机制可以为物联网带来更灵活可靠的权限控制。

2. 解决方案

物联网平台层面：

针对上述问题，考虑在物联网 IoT 平台的基础上引入区块链部件和功能，提供 IoT+区块链的解决方案。基于区块链技术扩展原平台的开放能力和建立数据商店，推动物联网数据高速流转，从源头上突破当前发展的瓶颈，从而引领区块链应用逐步从单行业拓展到跨行业融合。IoT+区块链解决方案的总体架构图如 20 所示：

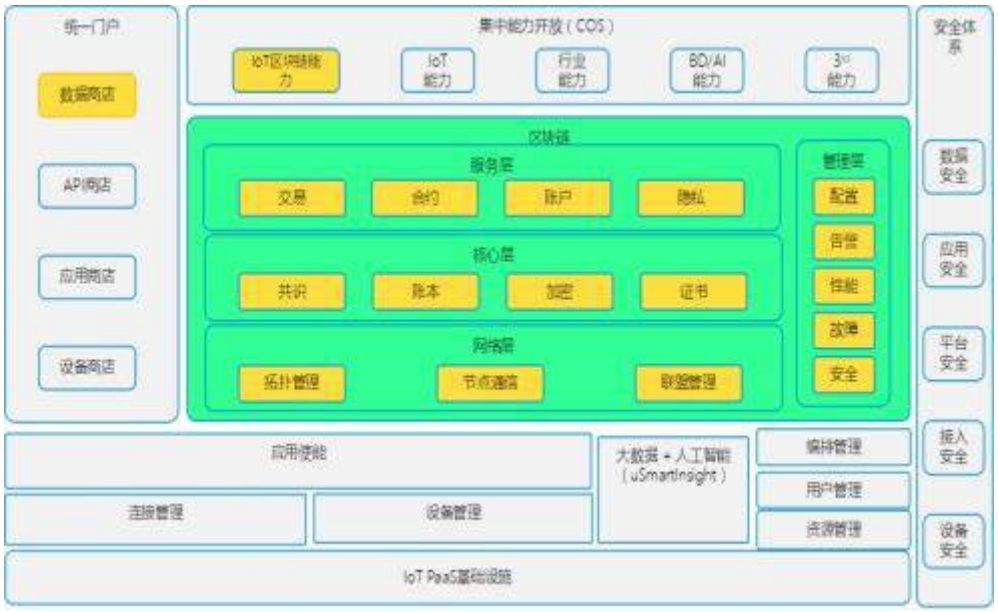


图 20 IoT+区块链解决方案的总体架构图

基于集成区块链技术， IoT 平台具备了区块链节点网络层、核心层、服务层功能，以及区块链管理功能，可为不同行业间数据提供了分享交换机制。IoT 平台区块链记录的数据，可采用统一的数据模型，保证数据在不同应用之间的理解一致，也给数据在各个物联网平台之间、以及物联网平台与应用之间的无障碍传递提供了便利。而物联网数据在上区块链之前，除了归一处理，还可经过清洗、脱敏、归约等操作，从而保证数据质量。IoT 平台可以支持以下典型的区块链数据记账流程图：

图 21 IoT 平台的区块链数据记账流程图

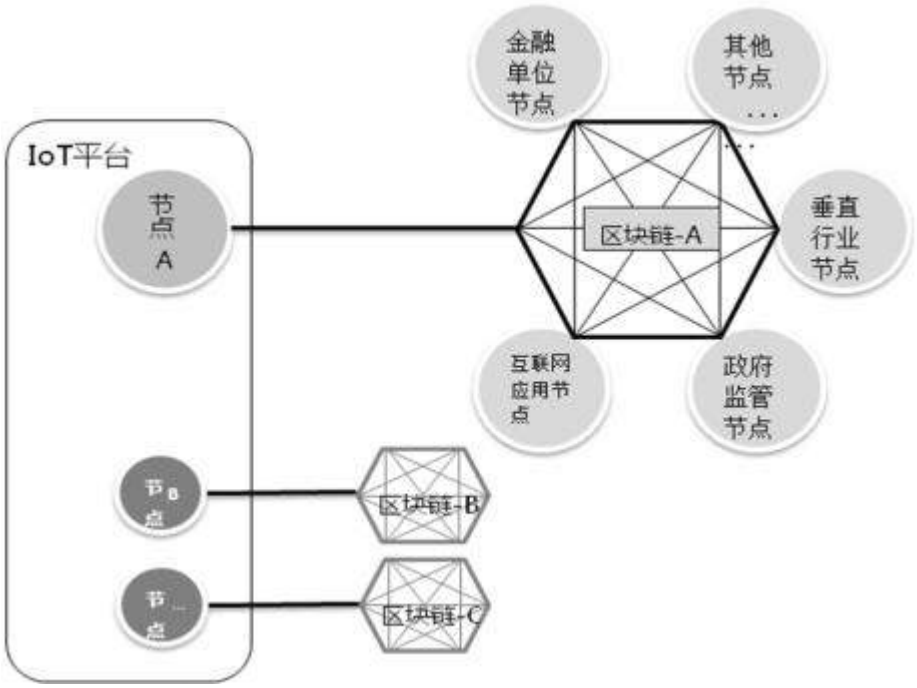


图 22 IoT 平台的区块链节点图

IoT 平台支持多个区块链网络，通过这种参与多区块链的组网模式，可以完成跨链交易。IoT 平台既可以提供区块链节点功能，也可以基于外置的区块链提供区块链数据访问功能。上述的数据清洗和映射，完成了数据归一化，从而保证不同区块链之间可以交换数据。

以上方案具备以下优势：

1) 完善的隐私安全保护

利用区块链记录数据指纹，加密机制和隐私授权机制保证用户隐私和数据资产安全。

2) 通过数据商店，促进数据高速流转

利用数据商店提供数据的存储、展示及共享一系列完整的功能，打造跨行业数据共享交换的应用平台，通过智能合约保证物联网区块链参与方收益，收益自动在参与方之间分成，挖掘并兑现数据的价值。

3) 通过能力开放，孵化融合应用

利用区块链能力开放，向包括终端、应用、其他平台方、互联网方等开放区块链的访问，并向其他平台和互联网厂家提供区块链融合的能力，简化了区块链应用开发流程，降低开发难度，从而促进融合应用的繁荣发展。

物联网应用场景方案：

针对四个典型场景进行区块链与物联网相结合的应用描述，映射不同的区块链类型以及区块链架构中，进而总结区块链与物联网在架构层面的融合方式。

（1）智能家居物联网

在智能家居网络中，许多不安全的设备（例如家用摄像机、智能灯、智能音箱等）容易被悄悄地劫持并变成肉鸡。被劫持的设备由恶意软件控制，对特定的服务器进行 DDoS 攻击。此外，设备存储数据的安全性也是使用者担忧的重点问题，特别是家用摄像机等拍摄的比较隐私的数据。

为了解决这些问题，可将区块链与智能家居网络相结合，组成一个私有链，示意图如下所示。

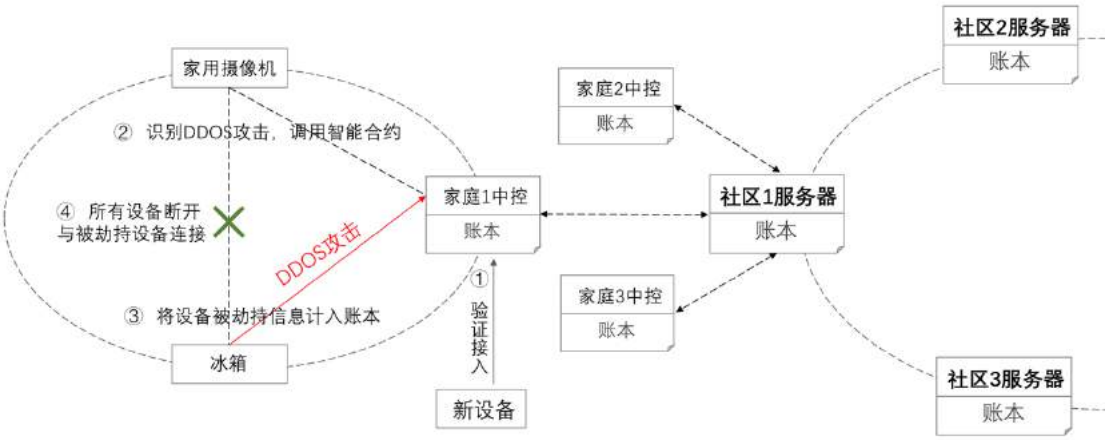


图 23 区块链与智能家居网络的结合

区块链的应用及其作用体现在：

①在新设备初次接入时，进行证书验证，以保证设备的可信性；

②当发现有设备被劫持时，将设备被劫持的信息记入账本，执行智能合约，禁止被劫持的家居设备连接到通信网络，即在连接到目标服务器之前切断其网络连接，以保证连接的可信性。

③家庭管理员排除被劫持设备安全隐患后，可通过私钥更新设备状态，恢复设备网络连接。此外，智能家居设备的数据（认证信息、配置参数、交互日志等）可被加密存储于账本中，只有私钥持有者才可查看，在实现数据云存储、云备份的同时，保障了数据的隐私性和安全性。

（2）环保物联网

环保是近年来国家关注的重点民生问题，切实关系到每个人的身体健康。将环保监测设备联网，组建“环保物联网”，是环保监管向着数字化、智能化，也向着精细化、规范化发展必经之路。环保物联网面临的主要问题有：

①数据的真实性。环保数据是否是真实的、能够反映实际情况，是环保物联网的基础。

②数据的安全性。环保数据可以被安全地存储，且不可被篡改，是环保物联网的保障。

③数据的权限控制。环保数据能否根据实际监管需求，灵活地配置各部门的权限范围，是环保物联网能否被广泛应用的关键。

为了解决以上问题，可将区块链与环保物联网相结合，组成一个联盟链，示意图如下。

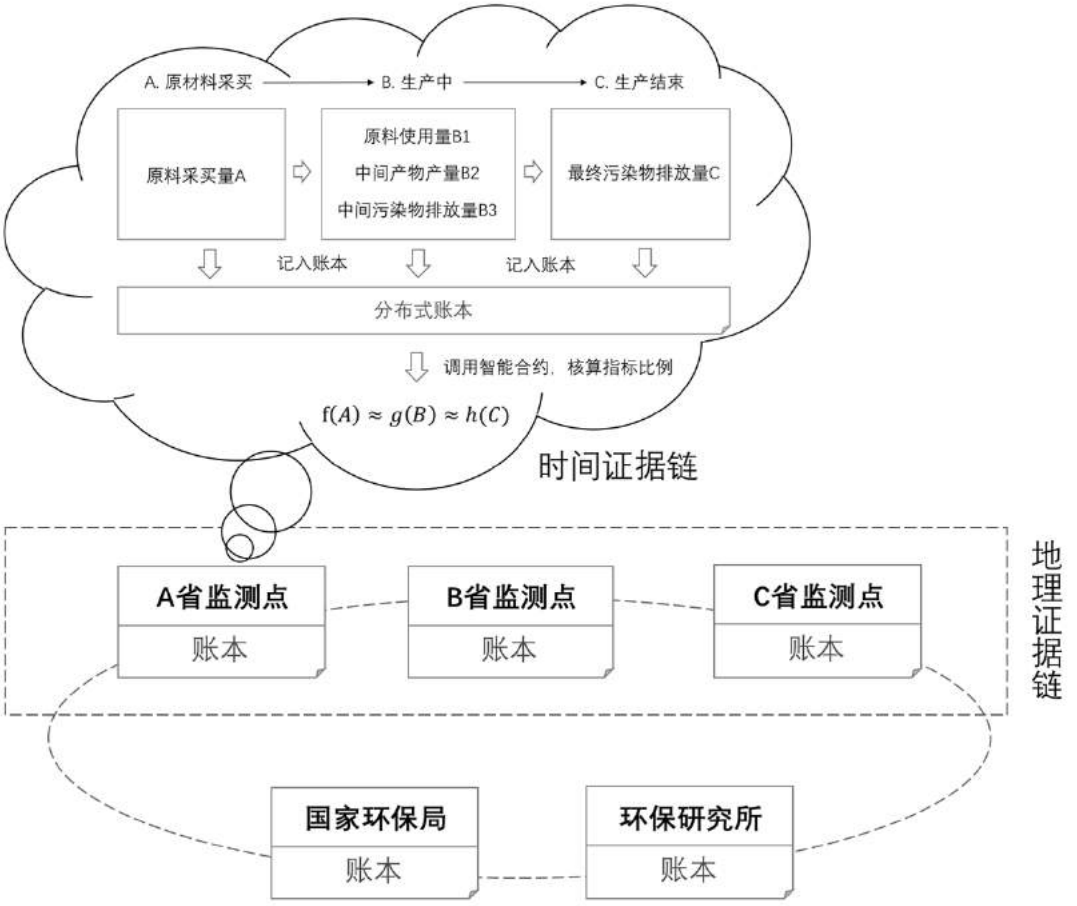


图 24 区块链与环保物联网相结合的联盟链

区块链的应用及其作用体现在：

①将生产过程中各流程数据存储为“时间证据链”，利用区块链

的合约层，编写算法实时根据计算模型来核算各个环节的指标数据，验证数据的合理性。例如：记录制造型企业通过物联网设备采集到的原料供应量（供应链）、原料使用量、中间产物产量、中间污染物排放量、最终污染物排放量，根据工厂使用的工艺，可以大致计算出这些指标值间的比例，如果有某个指标值异常，则这条链上的数据的真实性有待验证。

②将同一时刻各地区数据存储为“空间证据链”，利用区块链的合约层，编写算法实时根据模型核算各地区的指标数据，验证数据的合理性。例如：在 PM2.5 全面检测数据中，如果某个时点某地区周围的 PM2.5 值均较高，但是该地区的 PM2.5 数值很低，则该数据的真实性有待验证。

③区块链的不可篡改性，保证的数据的安全性。

④区块链可以根据权限，为每一个子网建立不同密钥加密的账本，从而为管理人员提供灵活的权限控制工具。

（3）车联网

车联网被认为是物联网体系中最有产业潜力、市场需求最明确的领域之一，其面临的主要问题有：

①车辆的接入成本。车联网具有较强的外部性，如何降低车辆的接入成本，将直接关系到车联网的价值创造能力。

②数据的有效同步。在大规模的网络中，如何保证每一辆车的数据都是完整同步的，是车联网面临的主要挑战之一。

③应用场景与激励机制。如何提高车主使用的积极性，增加车辆

联网设备的使用率，是车联网能够持久生存的关键。

为了解决以上问题，可将区块链与车联网相结合，组成一个公有链，示意图如下。

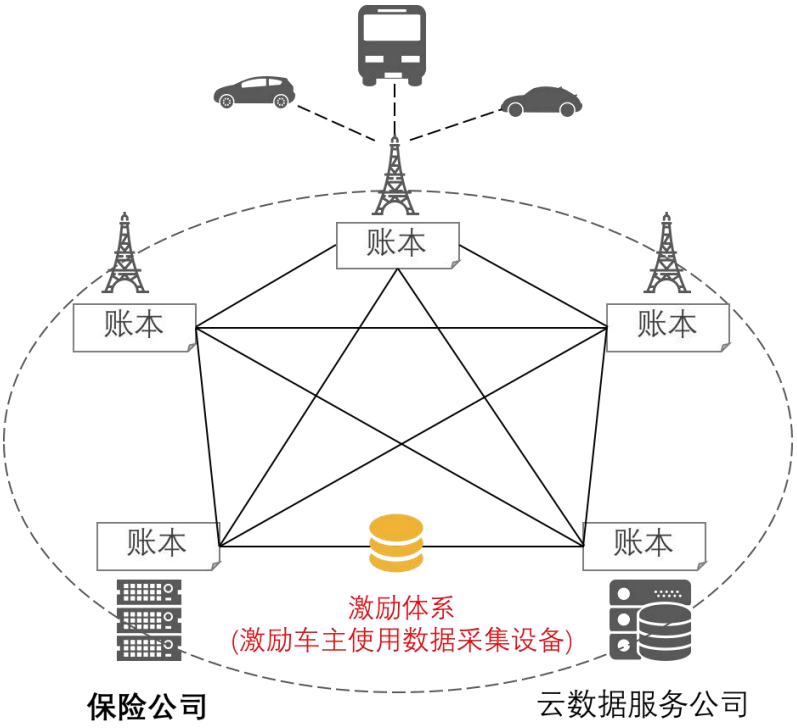


图 25 区块链与车联网相结合的公有链

区块链的应用及其作用体现在：

①通过区块链的网络层在各基站间建立可信连接，车辆就近与基站通讯，去中心化的架构可以有效降低新车辆的接入成本。

②通过区块链的网络层，在各基站间进行数据的传输，保证各个车辆状态数据的实时更新和完整性。

③通过区块链的激励层，根据数据上传量和在线时间为车辆发放奖励（例如可兑换的积分等），鼓励车主使用物联网设备，并为车辆提供状态云检测服务。

④车辆驾驶过程中产生的数据（如：时速、位置、状态等）将提

供给交通运营企业或保险公司，区块链的不可篡改性可以有效地保证数据的真实性。交通运营企业（公交集团、货运物流公司等）根据这些数据进行运力资源的实时调度和优化；保险公司以此进行保险计划制定、车辆事故定责定损、车辆保险赔付等服务。同时，为激励体系提供相应的兑付商品和服务，以激励车主客户使用和上传数据采集设备。

（4）机房租赁

2014 年，三大运营商共同出资成立中国铁塔公司。铁塔公司主要负责通信铁塔的建设、维护和运营，以及基站设备的代维。目前，基站机房主要由铁塔公司建立，出租给各大运营商，不同运营商的人往往需要进入同一个机房安装设备。机房租赁面临的主要问题有：

①机房出入较为频繁，出入手续较为复杂。

②多人进出机房，当发生意外情况时缺乏共识数据而发生纠纷。

为了解决以上问题，将具有人脸识别功能的智能门锁联网，组成一个由铁塔公司监管的联盟链，示意图如下。

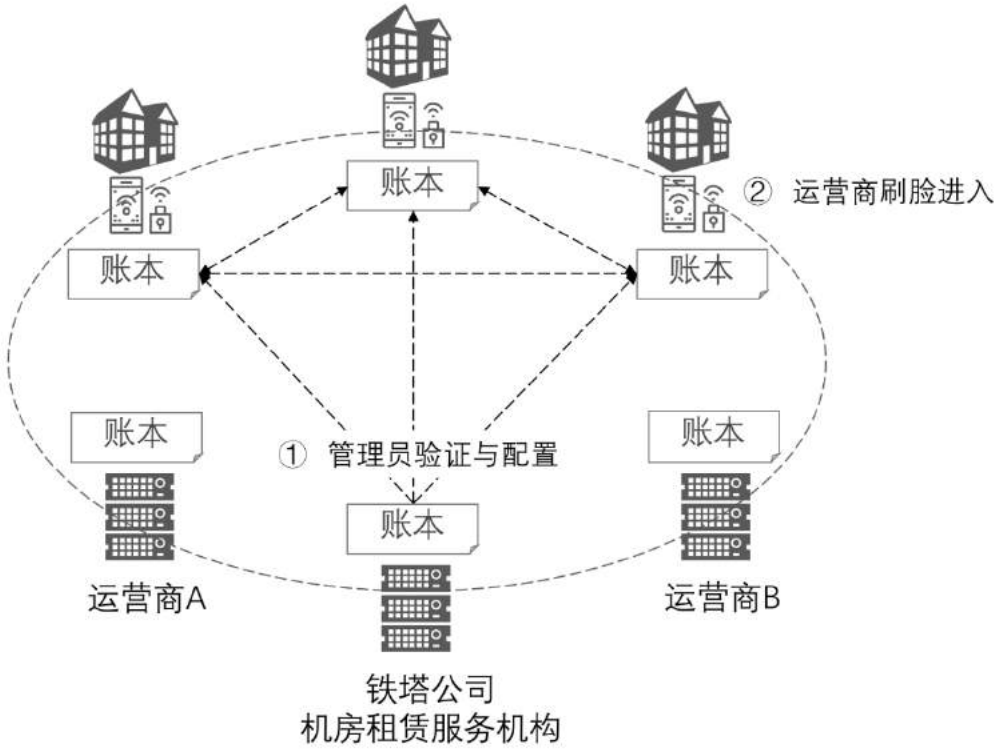


图 26 由铁塔公司监管的联盟链

区块链的应用及其作用体现在：

①加密存储机房、租赁关系、运营商维护人员信息，保证数据的不可篡改、实时更新和完整性。

②铁塔公司管理员持有私钥，进而获得分配机房使用权的权利，可以设置某人在某个时间段开启门锁。

③运营商维护人员可直接刷脸进入，方便快捷。

④存储每个机房的人员出入明细记录，为意外事故发生追责提供依据。

3. 发展策略

电信企业拥有海量的用户数据信息，使其在物联网领域拥有天然的优势，无可质疑地应积极响应区块链+物联网的时代号召，引入最前沿的区块链技术，巩固电信行业在物联网领域的龙头地位。

电信企业首先应当踊跃将区块链技术与本身业务相结合，管理物联网卡滥用的乱象，通过区块链数据的可追溯性优化物联网卡的监督管理工作；作为海量物联网数据的拥有者，电信企业应利用区块链的特性，实现物联网的数据源安全和信息交互安全，并为当前普遍存在的数据孤岛问题提供了解决思路；此外，电信企业还应当发挥自身技术优势，将区块链物联网系统与民生息息相关的领域，如医疗、农业、供应链管理等物联网应用积极结合，帮助各行业进行产业结构革新，努力推动社会生产力发展。

（七）云网融合

1. 发展现状

相对全球互联网的良好互连互通和高性价比的体验，运营商网络的区域特征明显，长期以来互连互通难度大，成本高，实施时间长，客户体验很受限。其中最大的三个障碍是：用户 3A(认证/鉴权/计费)，互连互通，费用结算；这三项都有望结合区块链而得到巨大改进。再结合 AI 的智能化自动化推进，有可能实现全球云网合一。区块链提供一种在不可信环境中，进行信息与价值传递交换的机制，是构建未来价值互联网的基石。以区块链助力运营商云网协同，打通全球云网资源，实现类互联网的泛在接入，以前所未有的高性价比支撑随需 SLA（SERVICE LEVEL AGREEMENT）。

2. 解决方案

跨网对接：以区块链跟踪网络设备/模块，结合 AI 实现快速互连

互通在电信业务和云业务走向全球化时，跨网对接，即网络互连互通互计费，成为一大障碍。传统意义上的网络互连互通，技术繁琐，流程冗长，困难重重；互计费则要实施大量数据的转写，格式重构，并结合 SWIFT 这样“较贵”的国际结算组织付费。整体成本高昂。即使以带宽/网络租用的形式实施网络互连互通，考虑其带宽复用效率，仍有大量的成本浪费。并由此导致基于网际互通的业务性价比，反而比不过 SD-WAN 这样协议层次更高但更灵活的方案。

结合区块链技术，可以跟踪到每一台设备，每一块板卡，每一个光模块，结合 AI 技术和海量数据库，有可能基于 AI 训练出的算法加上生产/实时监测数据实现模块/板卡/设备级别的互连互通，并实时记录互连互通的性能与故障，为协作的责任区分提供支撑，明确双方责任。这个方案，需要基于区块链标识海量硬件及期参数，标识海量软件/AI 模块及历史链，用以替代当前替代人工和简单测试系统的海量工作。这会是一个逐步推进的过程，相对于当前简单的硬性统一标准更具灵活性，更利于走向世界。

跨云对接：以区块链跟踪各云行为和接口，结合 AI 实现云间协同

与跨网对接相比，跨云对接，重在数据吞吐的可信的自动海量记录。这种吞吐已难以通过人工或传统的 BSS 系统及第三方来管控，而必需在双方可信的基础上实现真实记录，并应其海量的特点要求极低的记录与交互成本。对于上述这点，区块链是一种较好的解决方案。并且通过这些基于区块链的记录，运用 AI 可计算出单个云在一段时间内的对外特征，为云间协同及结算提供可信依据。结合各个云的可

信行为特征，在实施跨云对接时，可以结合 AI 实施策略组合和优选，以牵引各云的健康竞争，推进行业健康发展；同时，这些可信行为特征还可为各个云持续调整优化自身，明确发展目标提供较为确切的输入。对于企业自身运用的私有云和混合云尤其如此。

多云多网协同：以区块链跟踪客户行为和资源耗费，实现低成本实时结算

在全球化的大背景下，面临多云多网，如何选择组合以为用户实现最优性价比会成为一大挑战。这就要需要跟踪或分析客户行为和相应的资源耗费，并能支撑低成本的实时结算，以充分利用各云各网在不同时段的业务涨落和资费策略。此时，以区块链来标识用户和网络行为；以区域链来实现多云多网间的可信实时计算，都成为业务运营的基本要求。

云网合一：企业/个人用户以最简洁方式获取网络服务

根据英国电信（BT）对企业客户的调研显示，90%的企业希望能获得“云网一体化”的服务，以保障端到端的 SLA、安全 ，获取端到端的性能报告、实现端到端的管理和故障诊断能力。云网系统需要支持从任意一个云服务或者网络业务的销售入口登入，可以购买到任意一家的云服务或网络业务的功能，而不用多次登录不同的入口。

基于以上诉求，我们可以设计一种基于联盟链的云网业务方案：对联盟内企业进行“多云+多网”的销售进行授权认证，对云和网的销售记录、配置情况进行记账和追溯。以云服务侧购买网络为例：云服务侧向区块链提交购买/配置信息请求，而网络服务侧验证请求并

确认请求，云服务和网络服务侧达成共识并写入区块链，至此购买成功。在结算上，可根据区块链上的购买信息、配置更改信息、使用信息进行结算，同时保证账本的一致性，并支持实时结算。

3. 发展策略

对于云网融合中的区块链应用，首先是重点解决服务交易可信的问题，实现多云多网间从认证到收费的商业协同问题，如下图 17 所示：

图 27 多云多网间从认证到收费的商业协同问题

其中的各项改进点需要通过相应的商业联盟和生态组织共同策划，推动发展，集合国内各方面能力，尽快在国内生成适于云网融合的区域链技术和协议版本，借助国内高速发展的云服务和电信网络高速迭代，待成型后，再进一步向海外共享，推进全球云网协作。

其次，在多云多网协同时，会涉及多个厂商，运用区块链技术保证各厂商的产品可信也是需要重点关注的，如下图 28 所示：

图 28 基于区块链技术保证各厂商的产品可信

国内云网厂商的软件能力差别较大，在产品可信方向更加如此；部分厂商已有重点投资改进计划，可由先期实践的若干厂商提出区块链技术的可信应用场景，再发动国内相关专家做专项分析，以在产业内形成有共识的，可相互校验的区域链可信机制。

第三，区块链是一种致力于解决分布式安全可信性的新技术，需要针对电信中的云网协同做相应改造。其中 AES256 算法在未来会随着超级计算机的应用，甚至光子或量子计算机的应用，面临越来越大的挑战。至于在多长时间内能有效应对各种类似棱镜的窥探计划，需要考量。这个算法本身应该是相对独立，可以被单独设置和演进。另一个云网相互验证的问题，区块链上也要支持多层多重的区域划分，以将使用和认证范围限制在合理合法的范围内。并且需要将政府公信部门等也做为区块链的一分子，一起跟踪记录。此外，云网协同对区块链的计算速度和时延设置问题也有要求，即要能在较短时间内快速处理，还要能设置一定长度的时延，确保在这段时间内，变化可以有效被周边用户感知和记录。对于移动和家庭用户，这一点更为重要。

根深才能叶茂，希望下一步，能集合各领域力量，对这些做深度的适合中国国情的升级，以获得象中国高铁一样高品质，高性价比的解决方案。与此同时，区域链信息的存放与分发，也需要结合云，安全防护等因素，构建一个透明开放的模型，以利于各方面试验对接。

（八）多接入边缘计算

1. 发展现状

随着通信网络技术的发展，很多业务对宽带、时延等都提出了新的要求。为了提升用户体验，未来很多海量的数据都需进行本地化处理，这样可以降低网络负荷，并能获得更低的时延。多接入边缘计算技术（Multi-AccessEdgeComputing，下文简称 MEC）是近几年随着 5G 技术日趋成熟而兴起的研究方向。

MEC 可以看作是一个运行在移动网络边缘的、运行特定任务的服务器。其采用边缘计算技术，将 MEC 服务平台部署在网络边缘，可以极大缩短终端和应用服务器之间的传输路径，获得更低的时延，降低回传网络压力，从而可以有效提升用户体验。从另一个角度看，MEC 可以起到分流业务、凝聚价值的作用，运营商可提供基于 MEC 的各项业务，渗透到客户应用层面，可以有效避免移动网络被彻底管道化的威胁。MEC 常见的应用场景如下图 29 所示：

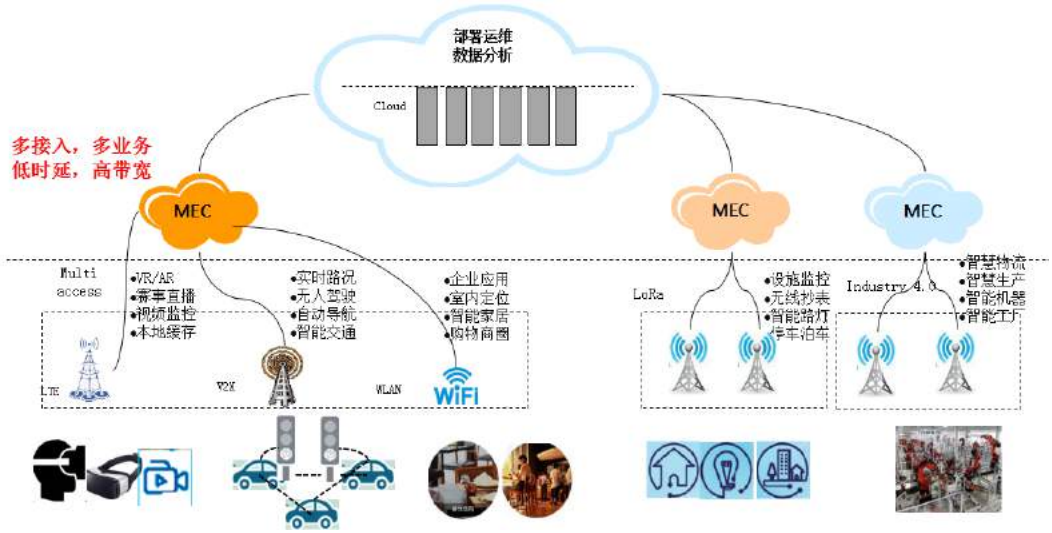


图 29 MEC 常见的应用场景

4G 时代，MEC 已经开始商用，并逐渐凸显出价值。在未来的 5G 时代，MEC 会得到更加广泛的应用，很可能会产生新的价值链、新的细分市场，很可能在技术及商业生态上带来新一轮的变革和颠覆。在电信蜂窝网络中，MEC 可以部署于无线接入网与移动核心网之间，可应用于多种通信场景。上图展示了 MEC 的一些应用场景，其中部分场景已开始商用。研究区块链与 MEC 应用场景的结合，将 MEC 所具有的资源和能力实现开放、共享和变现，可以为运营商挖掘和拓展全新的业务领域。区块链技术，可以提供交易的可追溯和不可篡改等特性，体现公平公正，提高用户参与的积极性，从而激发和促进 MEC 应用场景的规模部署。

2. 解决方案

MEC 与区块链的结合，技术上采用联盟链将更加高效，也可更好地满足监管、审计的需要。在实际部署中，区块链平台或应用可以安装部署在 MEC 服务器上，为不同的应用场景提供区块链技术和能力支

撑。在实际应用场景中，各个节点的角色不同，设想的角色功能如下：

- MEC 是管理节点，除可以写入区块链，还负责链上其它节点的注册、上线管理并设置相应的区块链访问权限，以及提供审计入口
- 各个注册的网络服务商、实体商家也被赋予写入数据的权限（或有选择性地赋予写入数据的权限）
- 普通移动用户，可以发起交易，可以查看区块中与自身相关的数据（或者被授权查看其它数据）

以下是区块链和 MEC 相结合的部分场景介绍：

2.1 MEC+区块链的存储与算力共享

在移动网络边缘的 MEC，因为机房、环境等条件限制，MEC 的硬件资源往往比较受限，而在 MEC 周边有一些设备具有较强处理能力，如手机/摄像头/个人电脑等，这些资源可能被利用起来强化 MEC 的能力。MEC 连接的本地网络服务器，或是本地网络中的一些个人电脑，均有一定的存储、算力资源。利用区块链技术，可以汇聚闲置的各类资源构建“无限节点”的资源网络，从而聚合成一个强大的资源池，并对分布在各节点的资源进行最优化的实时部署利用，这样可以有效地帮助 MEC 部署方节约成本和提高效率。MEC 的区块链技术的结合，可以提供丰富的算力等资源，进行共享，用于视频直播、本地缓存等业务，GPU 资源也可以用于 AI 训练等。

MEC 的运营者可以采用链上积分或链下支付的方式进行回报。交易后 MEC 可以操作使用接入区块链上的相应的资源。

MEC+区块链的资源共享示例图如下图 30 所示：

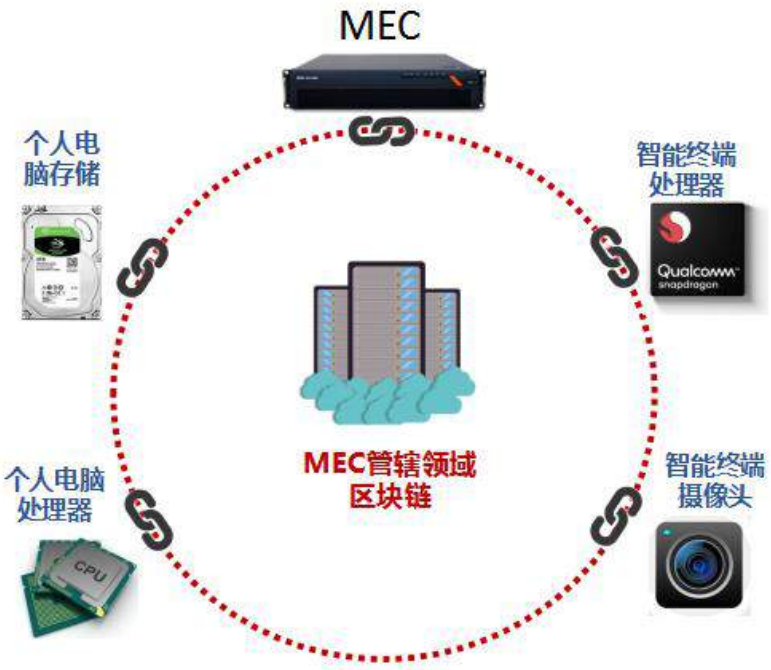


图 30 MEC+区块链的资源共享示例图

下文给出了处理流程的样例：

1）移动用户在设备上安装所需软件，将设备信息上报到 MEC，包括设备类型、资源配置、使用情况等，由 MEC 将其记录在链上。固定设备的信息发送到链上进行登记。

2）MEC 根据自身资源情况，或由运营者操作，使用其它设备的共享资源进行业务处理，将具体资源使用情况的数据放到链上，并给予共享设备者一定的积分奖励，记录到链上。

3）用户在购买 MEC 区块链范围内业务/产品时，可选择使用积分兑换，积分使用情况记录在区块链上。

基于区块链的特点，该场景实现了弱中心化的微服务和异步任务执行。同时，可以更进一步设想新的商业模式：计算资源需求方可把

希望执行的任务发布出来，任务被分割成碎片派发给 MEC+区块链链上的计算资源贡献者，贡献者执行碎片任务，获取相应奖励报酬，形成闭环。借助智能合约，MEC+区块链在资源提供方和资源需求方之间架起了桥梁。

2.2 MEC+区块链的车位资源共享

众所周知，很多一线、二线重点城市的车位是十分紧张的，特别是市中心的车位更加稀缺。但市中心某些固定停车位或者小区的车位，白天或者短时间内又是空闲的，空闲的车位无法得到有效利用，无形之中增加了各种社会成本和矛盾。而实现车位资源共享方案的一个难点就是无法有效地进行车位状态跟踪，同时也没有相应的费用分享机制，所以目前一直没有十分有效的车位资源共享方案。

当前，业界利用皮基站技术，已经可以实现车辆、车位的寻车功能，如果借助区块链的技术，可以很好地实现车位的资源共享：停车位可以作为一种资源进行交易，从而在车库管理方和车主之间，以及车主与车主之间借助于区块链，可以进行车位预定使用和转让等交易。

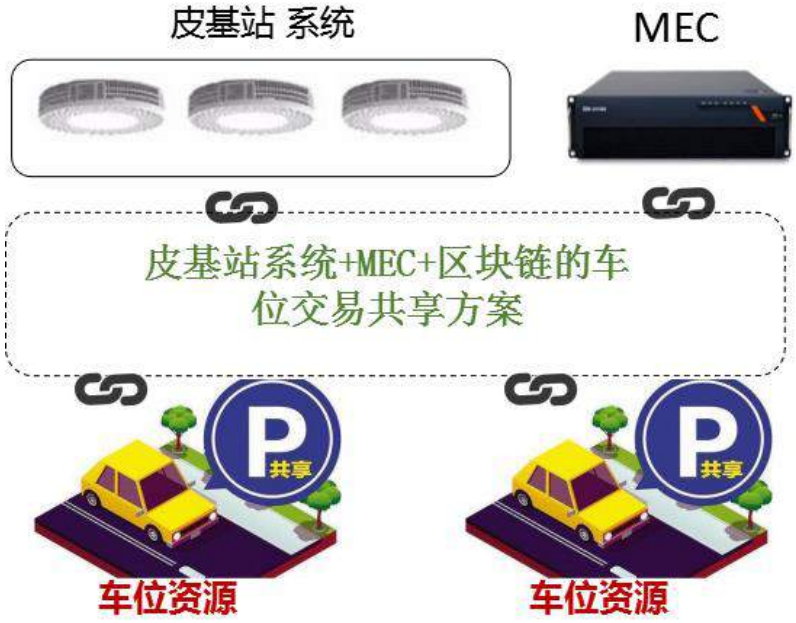


图31 基于区块链的车位交易系统

用户可以将空闲的车位发布到基于区块链的车位交易系统，进行车位的定时租赁，不但解决了停车难，也实现了资源的最大化利用。如果配合基于车位的物联网设备，甚至可以通过智能合约实现车位与租赁时间，费用的自动执行，人力成本、商务纠纷等都会大大下降。

3. 发展策略

新业务的爆炸式发展将驱动网络技术的不断演进。5G时代，万物互联、超低时延、超高带宽业务将成为网络演进的驱动力。利用部署于网络边缘的MEC服务器，移动运营商可实现移动业务的下沉，从而提高其业务分发、传送能力，进一步减少时延，并有效抑制核心网络内的拥塞产生，有助于提升现有移动应用的体验及移动网络的价值，未来市场的应用空间十分广阔。

未来MEC商用、试商用场景会越来越多，运营商需要在这些新领域中，拓展和获取新的运营收入。移动业务的下沉，势必会产生新的

需求，比如新业务的计费模式、复杂业务场景下的用户身份认证等，而区块链利用自身独特公平、公正、可信和不可篡改的技术优势，可以很好地为这些新业务场景提供解决方案，并将催生出更多全新的商业模式。

对于未来的发展，建议如下：

1) 推动区块链平台、应用部署在MEC服务器上

随着MEC的逐步商用，为了使区块链技术尽快在MEC场景中实现落地，运营商和设备商需提前考虑将区块链平台/应用部署在MEC服务器上，并进行功能、性能、稳定性和安全性相关的测试，为后续的场景落地做好充足准备。

2) 积极探索商用、试商用场景

运营商和设备商都需积极挖掘区块链与MEC业务相结合的场景，推动区块链和MEC相结合场景下的商用、试商用，使区块链技术可以更好地为MEC业务提供有效支撑。